

Addendum to Notification Materials

To: Maryland Office of the Attorney General

Re: eCapital Corp – Data Security Incident

Prepared by:

Mendes & Mount LLP on behalf of eCapital Corp.

Contact Information:

Margaret Reetz margaret.reetz@mendes.com (212) 261-8726

Gregory Mantych gregory.mantych@mendes.com (212) 261-8091

Incident Background

On July 22, 2021, eCapital discovered suspicious activity occurring on its systems (.e.g. machines shutting down; servers encrypted; eCapital's security software detecting ransomware activity). On the same day is discovered the incident, eCapital immediately engaged an external digital forensics firm to launch an investigation to determine the scope of the incident. eCapital also engaged Mendes & Mount, LLP (as US legal counsel) and Norton Rose Fulbright Canada LLP (as Canadian legal counsel) to coordinate a response.

The forensic investigation revealed that the earliest evidence of suspicious activity was noted on eCapital's network on April 25, 2021 when an administrative account was observed logging into a device through an unauthorized IP address. The initial point of entry was not confirmed.

On July 27, 2021, while investigations were ongoing, the external actor gained access to two eCapital email accounts through a phishing email. On July 29, 2021 the external actor sent unauthorized emails from the compromised users' accounts to eCapital's IT personnel and the incident response teams to pressure eCapital into negotiating a payment. All recipients identified the email as spam.

On or around August 6, 2021, eCapital was contacted by the Federal Bureau of Investigation to assist with its investigation and eCapital has been cooperating accordingly.

On August 17, 2021, the external actor gained access to a third eCapital email account through a phishing email. On August 19, 2021, unauthorized emails were subsequently sent to both internal and external eCapital contacts. On August 27, 2021, eCapital notified all recipients that the email received on August 19th was not legitimate and to avoid responding or clicking on any links contained therein.

Following the conclusion of the investigation, eCapital learned that the external actor had may have viewed and acquired various files from its network. The identity of the unauthorized third party remains unknown.

Remediation

eCapital immediately isolated and contained the incident upon discovery and engaged an external digital forensics firm to determine the scope and impact of the incident. The investigation found

evidence that an unauthorized third party accessed and may have acquired certain personal information.

In the intervening months, continued forensic analysis ensued and a data mining vendor was used to ascertain any potential individuals that may have been impacted because of this incident. eCapital worked continuously through a rigorous review of its files to identify the names and addresses of all individuals at issue. Through this exhaustive exercise, eCapital was able to provide contact information for every single individual to ensure that they received a direct notification with this information as well as remediation services.

On June 27, 2022, eCapital completed a review of the potentially impacted data to identify individuals whose information may have been involved and to gather up-to-date address information for notification purposes. After further review and through working with counsel and outside vendors, notification letters are to be mailed out August 8, 2022.

eCapital arranged for a toll-free call center through Experian to assist with answering questions about the incident and enrolling notified individuals in credit monitoring services. While eCapital is not aware of the misuse of any personal information as a result of this incident, out of an abundance of caution, eCapital offered complimentary credit monitoring services to all notified individuals through Experian for a period of 12 months (or 24 months where applicable). Again, through eCapital's exhaustive identification work, it was able to provide contact information for every individual to ensure that they received a direct notification with this information as well as these complimentary remediation services.

eCapital found no evidence that the personal information at issue has been misused by the unauthorized third party. It is out of an abundance of caution that credit monitoring has been offered to all potentially affected individuals to further minimize any risk of identity theft or fraud.

Number of Maryland Residents being Notified: 34



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

i1041-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345



SAMPLE A SAMPLE - L01 US NO MA CT DC
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789



NOTICE OF DATA BREACH

August 8, 2022

Dear Sample A. Sample,

We are writing to make you aware of an incident involving a potential exposure of your personal information. Below you will find details of the incident, steps eCapital Corp. ("eCapital") has taken to protect your information, and measures we are taking to help protect your personal information and prevent similar incidents going forward.

What Happened

On July 22, 2021, eCapital became aware that an unauthorized individual gained access to its network. The incident was unrelated to your account, and we are notifying you out of an abundance of caution. We are not aware of any misuse of your information.

What Information Was Involved

The information accessed contained information gathered as part of normal business operations, which we recently determined in some cases may have included individuals' names plus one or more of the following: Social Security number, driver's license number, and/or passport number.

What We Are Doing

eCapital immediately took steps to block the unauthorized access, evaluated security measures to prevent similar attempts in the future, and retained the services of an outside forensic vendor to investigate the incident.

We established a dedicated member support hotline to help address any further questions you may have about the incident at (800) 357-0823.

We engaged Experian to provide credit monitoring services at no cost to you. Details of this are below.



What You Can Do

We recommend reviewing the enclosed information outlining steps you can take to protect your information.

As an additional protection, we are providing access to Experian's® IdentityWorksSM identity and credit monitoring service at no cost to you. To activate the service and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: October 31, 2022** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (800) 357-0823 by **October 31, 2022**. Be prepared to provide engagement number B052227 as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH 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.

For More Information

If you have any questions regarding this incident, please contact the dedicated member support hotline at (800) 357-0823.

Sincerely,

eCapital Security Team

* 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.

Steps You Can Take to Further Protect Your Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and 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 also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Request a Copy of Your Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com>, calling toll-free 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 <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. Or you can 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 provided below:

Equifax
800-685-1111
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
888-397-3742
www.experian.com
535 Anton Blvd., Suite 100
Costa Mesa, CA 92626

TransUnion
800-916-8800
www.transunion.com
P.O. Box 6790
Fullerton, CA 92834



Place a Fraud Alert

You may consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Institute a Security Freeze

You may have the right to put 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 a freeze. A credit freeze 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. There shall be no charge for a security freeze. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Please contact the three major credit reporting companies as specified below to find out more information:

Equifax: P.O. Box 105788, Atlanta, GA 30348, www.equifax.com

Experian: P.O. Box 9554, Allen, TX 75013, www.experian.com

TransUnion LLC: P.O. Box 2000, Chester, PA, 19022-2000, freeze.transunion.com

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: 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, the addresses where you have lived over the prior five years; 5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed; 6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); 7. Social Security Card, pay stub, or W2; 8. 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.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed above. The contact information for the Federal Trade Commission is as follows:

Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/idtheft
877-ID-THEFT (877-438-4338)

For Maryland residents: The contact information for the state Attorney General's office is as follows:

Maryland Office of the Attorney General, Consumer Protection Division
200 St. Paul Place, Baltimore, MD 21202
888-743-0023 toll-free
<https://www.marylandattorneygeneral.gov>

For New York residents: The contact information for the state Attorney General's office is as follows:

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
800-771-775
<http://ag.ny.gov>

For North Carolina residents: The contact information for the state Attorney General's office is as follows:

North Carolina Attorney General
114 West Edenton Street
Raleigh, NC 27603
919-716-6400
<https://ncdoj.gov/>

For Rhode Island residents: The contact information for the state Attorney General's office is as follows:

Office of the Attorney General
150 South Main Street
Providence, Rhode Island 02903
401-274-4400
<http://riag.ri.gov>

Right to Obtain a Police Report

For Massachusetts and Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

Additional Free Resources on Identity Theft

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit <http://www.ftc.gov/idtheft> or call 1-877-ID-THEFT (877-438-4338).



