



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

March 22, 2023

Bruce A. Radke
(312) 463-6211
bradke@polsinelli.com

VIA E-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, Maryland 21202

Re: Notification of a Potential Data Security Incident

Dear Mr. Karberg:

We represent Johns Hopkins Federal Credit Union (“JHFCU”), 2027 E. Monument Street Baltimore, MD 21205, in connection with a recent incident that may have involved the personal information of three hundred sixty-eight (368) Maryland residents. We are reporting a potential data security incident 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 JHFCU is notifying you of this incident, JHFCU does not waive any rights or defenses relating to the incident or this notice.

NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS

On March 2, 2023, JHFCU discovered that a skimmer device that was capable of capturing card information was installed on an ATM at 5201 Alpha Commons Drive Baltimore, MD 21224. On March 6, 2023, while reviewing video security footage, JHFCU learned a second skimmer device was installed on an ATM at 4 East 33rd Street Baltimore, MD 21218. JHFCU determined both skimmers were installed on the ATMs from February 26, 2023 through March 2, 2023. JHFCU’s investigation determined that the skimmers captured cardholder information for individuals who used the ATM during the window of time the skimmers were installed. The information included name, card number, expiration date, service code and CVV number. JHFCU reported these incidents to law enforcement, and understands the investigation is ongoing.

NUMBER OF MARYLAND RESIDENTS AFFECTED

JHFCU determined that the incident involved the personal information of three hundred sixty-eight (368) Maryland residents. JHFCU mailed notification letters to the individual via USPS mail on March 22, 2023. This notice included a contact number that the individuals can call should they

polsinelli.com

Atlanta Boston Chicago Dallas Denver Houston Kansas City Los Angeles Nashville New York Phoenix
St. Louis San Francisco Seattle Washington, D.C. Wilmington

Polsinelli PC, Polsinelli LLP in California



March 22, 2023

Page 2

have questions or require assistance. A copy of the notices sent to the involved individuals is enclosed.

STEPS TAKEN RELATING TO THE INCIDENT

Upon learning of the incident, JHFCU confirmed the skimmers were removed from the ATMs, identified the involved members, and blocked and reissued the member cards. JHFCU notified FISERV and VISA regarding non-member cards. JHFCU also inspected its other ATMs for similar devices and found none. JHFCU notified law enforcement and continues to cooperate with the ongoing investigation. JHFCU is undertaking efforts to reduce the risk of a similar incident occurring in the future, including additional surveillance of its ATM machines. Finally, as discussed above, JHFCU is notifying individuals and providing them with information on how to protect against potentially 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.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Bruce A. Radke'.

Bruce A. Radke

Enclosure



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>>:

Johns Hopkins Federal Credit Union (“JHFCU”) values and respects the privacy of your information, which is why we are following up on the recent email or phone call from our Card Services team regarding your Card # ending in <<Breached Elements>>. We want to provide you with more information about the recent security incident involving that card, and guidance on what you can do to protect yourself, should you feel it is appropriate to do so.

What Happened? On March 2, 2023, we became aware that a skimmer device was installed on the ATM at the Bayview branch lobby location from February 26, 2023, through March 2, 2023. Our investigation determined that the skimmer captured cardholder information for individuals who used the ATM during the window of time the skimmer was installed. We have reported this incident to law enforcement, and we will continue to assist with their investigation.

What Information Was Involved? We are notifying you because your Card # ending in <<Breached Elements>> was used at the Bayview branch lobby ATM machine between February 26, 2023, and March 2, 2023. The information that could have been captured by the skimmer includes your name, card number, expiration date, service code and CVV number. The skimming device did not acquire your Social Security number, driver’s license number, address, phone number or any of your other financial information.

What We Are Doing. As you know, we blocked and reissued the debit card referenced in this letter. We continue to review our safeguards to protect member information, including additional surveillance of our ATM machines. Members who have experienced losses due to fraudulent transactions as a result of this incident will have their funds fully restored.

What You Can Do. Please let us know if you did not receive your new debit card, or if you are having any trouble activating the card. We encourage you to review the following information on steps to protect yourself against identity theft or fraud in the enclosed *Additional Important Information* sheet.

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 this incident might cause. For further information and assistance, please call 410-534-4500 or 1-800-543-2870 during normal business hours.

Sincerely,

Johns Hopkins Federal Credit Union

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.

Under Massachusetts law, 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.

Security Freezes: You may have the right to place a security freeze on your credit report. A security freeze can be placed without any 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.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below or, if available, comply with the consumer reporting agencies' online security freeze request procedures:

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

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

In order to request a security freeze, you may 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.); and
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.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus 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, you must call or send a written request to the credit reporting agencies by mail or, if available, comply with the consumer reporting agencies' online procedures for lifting a security freeze, 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail or, if available, comply with the consumer reporting agencies' online procedures for removing a security freeze, 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 three (3) business days after receiving your request to remove the security freeze.

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 <https://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 9554
Allen, TX 75013

TransUnion
1-800-888-4213
www.transunion.com
P.O. Box 1000
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.

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/bcftp_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.

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/>.