



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

S. Chandler Harris
Office: (267) 930-1290
Fax: (267) 930-4771
Email: charris@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

August 16, 2023

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent BankCard USA Merchant Services Inc. ("BankCard USA") located at 2625 Townsgate Rd #100, Thousand Oaks, CA 91361 and are writing to notify your office of an incident that may affect the security of certain personal information relating to one hundred ninety (190) Maryland residents. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, BankCard USA does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On June 1, 2023, BankCard USA discovered suspicious activity relating to their computer systems. They immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. The investigation determined that files on certain computer systems were subject to unauthorized access and acquisition between May 31, 2023 and June 1, 2023. BankCard USA began reviewing the affected systems to determine what, if any, sensitive information was contained within the systems in question. On July 14, 2023, BankCard USA confirmed the scope of that the information that could have been subject to unauthorized access includes name, Social Security number and financial account information of one hundred ninety (190) Maryland residents.

Notice to Maryland Residents

On August 16, 2023, BankCard USA provided written notice of this incident to one hundred ninety (190) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering the event, BankCard USA moved quickly to investigate and respond to the incident, assess the security of BankCard USA systems, and identify potentially affected individuals. Further, BankCard USA notified federal law enforcement regarding the event. BankCard USA is also working to implement additional safeguards and training to its employees. BankCard USA is providing access to credit monitoring services for twenty-four (24) months, through Equifax, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, BankCard USA is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. BankCard USA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

BankCard USA is providing written notice of this incident to relevant state regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-1290.

Very truly yours,

S. Chandler Harris of
MULLEN COUGHLIN LLC

SCH/kzm
Enclosure

EXHIBIT A



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

<<Name 1>>
<<Name 2>>
<<Address>>
<<City>>, <<State>> <<Zipcode>>

<<Date>>

<<VARIABLE DATA 2>>

Dear <<Name 1>> :

BankCard USA Merchant Services Inc. (“BankCard”) is writing to inform you of an incident that has impacted the security of some of your information. Although we have no indication of actual fraud or misuse of your information, we are providing you with information about the incident, our response to it, and resources available to you to help protect your information, should you feel it appropriate to do so.

What Happened? On June 1, 2023, we discovered suspicious activity relating to our computer systems. We immediately launched an investigation, with the assistance of third-party forensic specialists, to determine the nature and scope of the activity. Our investigation determined that files on certain computer systems were subject to unauthorized access and acquisition by an unauthorized party between May 31, 2023 and June 1, 2023. BankCard began reviewing the affected systems to determine what, if any, sensitive information was contained within the systems in question. On July 14, 2023, BankCard confirmed certain information related to you was contained within the files. We are notifying you and providing information about the incident, and resources to help protect your personal information.

What Information Was Involved? The following types of your information were identified in the files: your name and <<Consolidated Breached Elements>>.

What We Are Doing. BankCard takes the confidentiality, privacy, and security of information in our care very seriously. Upon discovery, BankCard immediately commenced an investigation to confirm the nature and scope of the incident. BankCard reported this incident to law enforcement, has implemented additional layers of security in our identification and verification processes, and is taking steps to implement additional safeguards and review policies and procedures relating to data privacy and security. As an added precaution, we are also offering you complimentary access to 24 months of credit monitoring and identity theft restoration services, through Equifax. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Information* for additional information on these services.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect errors. You may also review the information contained in the enclosed *Steps You Can Take to Help Protect Your Information*. There you will also find more information on the credit monitoring and identity restoration services we are making available to you. While BankCard will cover the cost of these services, you will need to complete the activation process. Enrollment instructions are included in this letter.

For More Information. BankCard understands you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, please call the dedicated assistance line at <<Variable Data 1>> (except U.S. holidays). You may also write to BankCard at 2625 Townsgate Road Ste 100 in Westlake Village, CA 91361.

Sincerely,

Shawn Skelton
President, BankCard USA Merchant Services, Inc.

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Monitoring Services

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 notifications¹ 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 alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- 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 theft⁴

Enrollment Instructions

Go to www.equifax.com/activate

Ensure that you enroll by <<**Enrollment Deadline**>> (Your code will not work after this date.)

Enter your unique Activation Code of <<**ACTIVATION CODE**>> 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.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.

For New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers’ files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit “prescreened” offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel

have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage consumers to review their rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, individuals have the right to obtain any police report filed in regard to this event. There are approximately <<RI Count>> Rhode Island residents that may be impacted by this event.