State Employees' Credit Union

[DATE]

[RECIPIENT NAME]
[RECIPIENT ADDRESS1]
[RECIPIENT ADDRESS2]

Re: Notice of Data Breach
Visa® Gift Card(s) Ending in: [XXXX] [XXXX] [XXXX] ("Gift Card(s)")

Dear [RECIPIENT NAME(S)]:

State Employees' Credit Union ("SECU" or "we") records indicate that you are the registered cardholder for the above-referenced Gift Card(s). We are writing to notify you of an incident involving PSCU Incorporated ("PSCU"), SECU's Gift Card service provider, and PSCU's vendors ("Vendors"). This letter describes the incident, what we are doing to address it, and how you can contact us for additional assistance.

What happened.

In mid-June 2023, PSCU informed SECU that a Vendor experienced a security incident involving personal information in May 2023. The incident affected the Vendor's computer systems that contained Gift Card account information. We are providing this notice because we determined that certain personal information associated with your Gift Card account was accessible to unauthorized parties as a result of the security incident.

What information was involved.

The personal information associated with your Gift Card account that was affected by this incident may have included your Gift Card account number and card verification code for your Gift Card, as well as the name, date of birth, address, e-mail address, and telephone number that you provided when you registered the Gift Card. To our knowledge, no other accounts or personal information were affected.

What we are doing.

SECU has closed the Gift Card(s), and we are continuing to investigate this incident with and through PSCU. SECU is also in the process of issuing refunds to cardholders, where applicable, totaling the amount of funds originally loaded on the Gift Card(s) minus the amount of any transactions our records reflect that you authorized prior to the closure.

What you can do.

If you have entered any Gift Card as a method of payment on any websites, you should remove it, since the card has been closed. You should remain vigilant, such as by regularly reviewing your account statements with all of your financial institutions over the next twelve to twenty-four months. If you are a credit union member, please report to us any activity associated with your accounts that you do not recognize. You may also choose to monitor your credit reports. The "Additional Resources" section of this letter describes additional steps you can take and provides

contact details for the Federal Trade Commission and credit reporting agencies, as well as information on how to place fraud alerts and security freezes.

For more information.
If you have questions or need additional assistance, please call 24/7 Member Services at any time at (888) 732-8562 or contact us using one of the methods described on our website at https://www.ncsecu.org/Home/ContactUs.html.

We regret this incident and apologize for any inconvenience or concern it caused.

Sincerely,
SECU Risk Management

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:
Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. We recommend you do so and have any information related to fraudulent transactions deleted.
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.

Fraud Alerts. There are two types of fraud alerts, both free of charge, 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 at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge. A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze: (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, and display your name, current mailing address, and the date of issue.

Federal Trade Commission. 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 home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft. Online guidance regarding steps you can take to protect against identity theft is available from the FTC at the website listed below.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).