FRAUD ALERT

ID Theft and Fraud
Avoid Becoming a Victim
What To Do If You Are a Victim
Resource Center

E-mail Scams

The alerts listed on this page are scams directed at residents in our region. If you receive an email, text message, or phone call similar to any of these listed, please forward it directly to Sun East at abuse@suneast.org. Text messages can be forwarded to 610-500-3462. Do not click on any links and do not respond to any requests in the email, message, or phone call. Sun East works closely with law enforcement to shut down any fraudulent websites or phone numbers once they are reported.

PHONE CALL FROM MASTERCARD OR VISA - LIVE PERSON

The scam is as follows:

You receive a phone call from MasterCard or VISA: Caller: 'This is (name), and I'm calling from the Security and Fraud Department at VISA. My Badge number is 12460. Your card has been flagged for an unusual purchase pattern, and I'm calling to verify. This would be on your VISA card which was issued by (name of bank). Did you purchase an Anti-Telemarketing Device for $497.99 from a Marketing company based in ?'

When you say 'No', the caller continues with, 'Then we will be issuing a credit to your account. This is a company we have been watching and the charges range from $297 to $497, just under the $500 purchase pattern that flags most cards. Before your next statement, the credit will be sent to (gives you your address), is that correct?'

You say 'yes'. The caller continues - 'I will be starting a Fraud investigation. If you have any questions, you should call the 1- 800 number listed on the back of your card (1-800 -VISA) and ask for Security.'

You will need to refer to this Control Number. The caller then gives you a 6 digit number. 'Do you need me to read it again?'

Here's the IMPORTANT part on how the scam works. The caller then says, 'I need to verify you are in possession of your card'. He'll ask you to 'turn your card over and look for some numbers'. There are 7 numbers; the first 4 are part of your card number, the next 3 are the security Numbers that verify you are the possessor of the card. These are the numbers you sometimes use to make Internet purchases to prove you have the card. The caller will ask you to read the 3 numbers to him. After you tell the caller the 3 numbers, he'll say, 'That is correct, I just needed to verify that the card has not been lost or stolen, and that you still have your card. Do you have any other questions?' After you say No, the caller then thanks you and states, 'Don't hesitate to call back if you do, and hangs up.

You actually say very little, and they never ask for or tell you the Card number. What the scammers want is the 3-digit PIN number on the back of the card. Don't give it to them!

APPROPRIATE ACTION: Tell the caller that you will call VISA or MasterCard directly for verification of their conversation. The real VISA will never ask for anything on the card as they already know the information since they issued the card! If you give the scammers your 3 Digit PIN Number, you think you're receiving a credit. However, by the time you get your statement you'll see charges for purchases you didn't make, and by then it's almost too late and/or more difficult to actually file a fraud report.

NEVER give out personal information over the phone, via text message or by email unless you initiated the contact and can verify the identity of the company or individual you are communicating with.

RECORDED PHONE MESSAGE SCAM ALERT as of October 2, 2009

As of this morning, Sun East was notified that individuals in our area are receiving recorded phone calls and voicemails claiming that their VISA Debit Card has been deactivated. The recording sounds very professional and asks for their 16-digit card number to reactivate the card. PLEASE DO NOT GIVE OUT YOUR CARD NUMBER OR PERSONAL INFORMATION. THIS IS A SCAM.

Sun East does not ever communicate important account information via phone, voicemail, recorded messages, or text messages. We have also stopped all promotional and email communications to our members.

If a message seems suspicious to you, please call **877-5-SUNEAST**! That is the only number you need to call to contact the Credit Union.

TEXT MESSAGE SCAM ALERT as of September 4, 2009

During the last few days text messages were circulated throughout our area requesting the receiver to call a fraudulent phone number. When the receiver calls that number they are greeted with the following message: *You have reached Sun East MasterCard Department. We have received many complaints about unauthorized charges. We will be reissuing new card numbers. Enter your 16 digit card number….."* THIS IS A SCAM.

PLEASE DO NOT call the phone number associated with this message and DO NOT enter your card number or any other personal information. Sun East does not contact our members via Text Message and we will never ask you for your account information using an automated attendant.

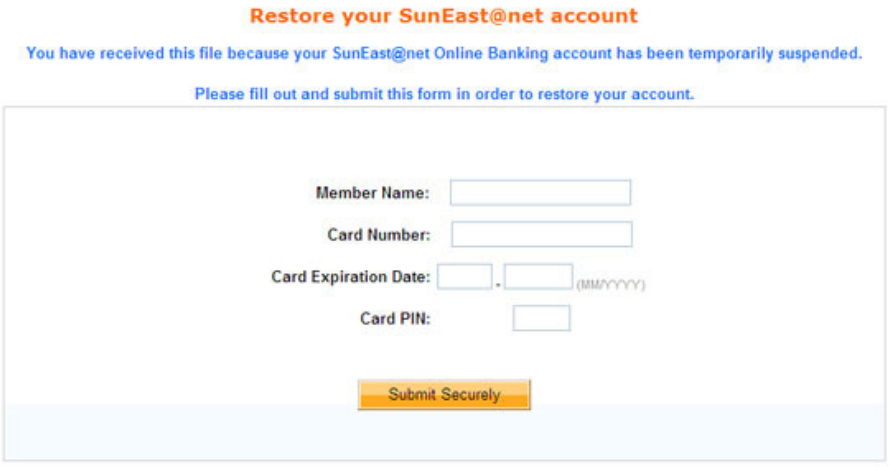
If a message seems suspicious to you, please call **877-5-SUNEAST**! That is the only number you need to call to contact the Credit Union.

TEXT MESSAGE SCAM ALERT as of August 24, 2009

Over the weekend, several text messages were circulated throughout our area with the following message: *Service center for your Sun East Federal Credit Union MasterCard/Debit Card account. Verify recent activity that has appeared on your account. Enter your card number followed by the pound sign.*

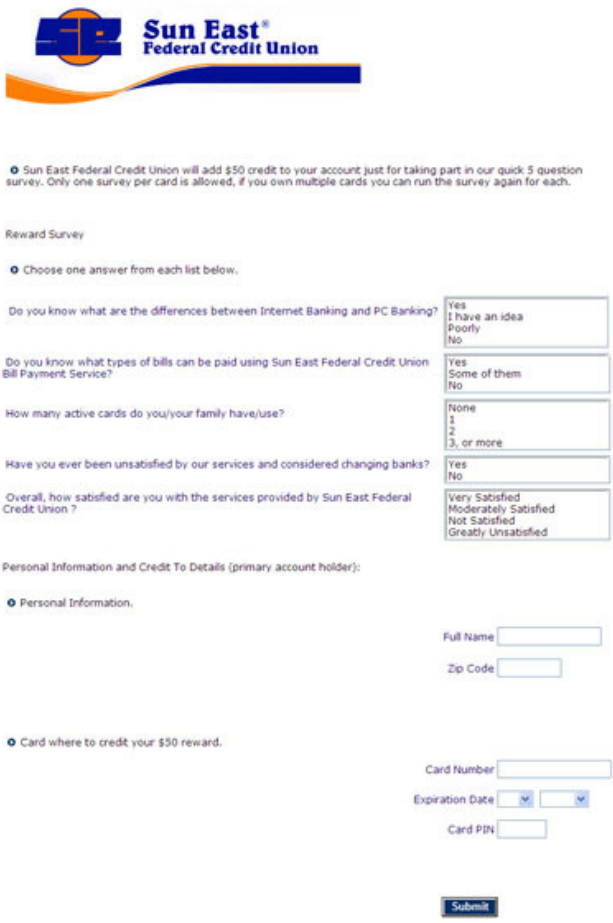
EMAIL SCAM ALERT as of August 11, 2009

The following email is currently circulating. This is NOT a Sun East generated email. Sun East will NEVER ask you for your personal account information by email. Please do not respond to this email and DO NOT enter any personal information.



EMAIL SCAM ALERT as of August 5, 2009

The following survey is being circulated by email. DO NOT take this survey. DO NOT respond in any way to this email. This is NOT A SUN EAST EMAIL. All surveys conducted by Sun East Federal Credit Union are sent through U.S. Mail.



Sun East Federal Credit Union

Sun East Federal Credit Union will add $50 credit to your account just for taking part in our quick 5 question survey. Only one survey per card is allowed, if you own multiple cards you can run the survey again for each.

Reward Survey

Choose one answer from each list below.

Do you know what are the differences between Internet Banking and PC Banking? — Yes / I have an idea / Poorly / No

Do you know what types of bills can be paid using Sun East Federal Credit Union Bill Payment Service? — Yes / Some of them / No

How many active cards do you/your family have/use? — None / 1 / 2 / 3, or more

Have you ever been unsatisfied by our services and considered changing banks? — Yes / No

Overall, how satisfied are you with the services provided by Sun East Federal Credit Union ? — Very Satisfied / Moderately Satisfied / Not Satisfied / Greatly Unsatisfied

Personal Information and Credit To Details (primary account holder):

Personal Information.

Full Name

Zip Code

Card where to credit your $50 reward.

Card Number

Expiration Date

Card PIN

Submit

TEXT MESSAGE SCAM ALERT as of July 13, 2009

Two separate phishing attempts were circulated in our area over the weekend via text message. These are Fraudulent Messages. Sun East does NOT communicate via text messages. The messages are below and the phone numbers associated with these messages have been shut down.

Message 1: SUN.EAST@suneast.org / Sun East F.C.U. Call us at 1-877-382-4627 regarding this SMS Alert (Notification). Thank you. /

Message 2: SunEast@suneast.org / SunEast F.C.U. Go Paperless - 5 Members Will Win $5,000. Ends 08/24/09. Call us at 1-877-278-0380/1-877-267-3334. Thank you. /

DO NOT CALL THESE NUMBERS. DO NOT ENTER YOUR ACCOUNT INFORMATION. Do not enter your account and pin numbers, and do not offer any personal information. Please report a text message you receive by forwarding it to Sun East at 610-500-3462. You can also report fraud to abuse@suneast.org or call 877-5-SUNEAST.

EMAIL SCAM ALERT as of April 30, 2009

A phishing attempt was recently sent out by email to both members and non-members. The link in the email directs them to a website that looks identical to Sun East's Home Banking login screen. However, if you notice in the address window, site is actually http://www.grundschule-vehlefanz.de/SunEast/login.htm. The real address for Sun East's Home Banking login screen is https://hb.suneast.org/.

DO NOT ENTER YOUR ACCOUNT INFORMATION. Do not enter your account and pin in to this screen and do not offer any personal information. If you receive an email from Sun East asking to verify your identity in any way, report it to abuse@suneast.org or call 877-5-SUNEAST.

TEXT MESSAGING SCAM ALERT as of February 27, 2009

We have received reports of area residents receiving text messages from someone claiming to be Sun East Federal Credit Union asking recipients to call an 800 number to verify account information. During the phone call, a recorded message asks a series of questions in order to obtain personal account information. This is a scam. Sun East FCU does not use text messaging capabilities to communicate with our members.

PHONE SCAM ALERT as of February 24, 2009

As of 5 pm last night, a large number of phone calls went out to residents in the Philadelphia area.

These were automated phone calls, that when answered, asked for a number of different pieces of secure information such as card numbers, pin's etc. The caller id phone numbers that showed up for these calls were manipulated to show that the calls were coming from legitimate places of business throughout the U.S. and Canada. DO NOT call the number that comes up on caller ID for any reason, these numbers were faked and the people on the other end are not responsible for the phishing calls.

TEXT MESSAGE ALERT as of January 9, 2009

Residents in the area are now receiving text messages stating that their Sun East card has been locked and that they should call either 800-801-8057 or 866-493-3588 to get it unlocked. Please do not call these numbers and do not respond to this message. THIS IS A SCAM.

Sun East currently does not notify members by sending text messages.

The individuals attempting to steal your information purchase a listing of cell phone numbers and use an automated machine to leave the text message. As with other phishing attempts, there has not been any leak of data from Sun East - these cell phone lists are available for purchase over the Internet and the vast majority of the recipients are not Sun East members.

The 800 and 866 numbers have been reported. Law enforcement agencies have been notified.

EMAIL ALERT as of December 4, 2008

The following email was sent across the region in the morning. As always, DO NOT call this number and DO NOT give out your personal information over the phone. Other phone numbers involved are in the 302, 303, and 713 area codes. Another email went out at 1:20 pm asking recipients to call 877-214-0565.

> This is not a promotional e-mail. Please call us immediately at 1-610-628-4034 regarding recent activity on your SunEast@ Debit Card.
>
> We're available 24/7 to take your call.
>
> Please disregard this e-mail if you've already call us since the date this e-mail was sent.
>
> We appreciate your prompt attention to this matter.
>
> Thank you
> Sun East Federal Credit Union

PHONE ALERT as of October 7, 2008

County residents are receiving automated phone calls soliciting personal account information. When they answer the phone they are told this is Sun East and your credit card has been deactivated, please press '1'. Through a series of prompts, individuals are asked to enter their account information. THIS IS A SCAM. DO

NOT enter any information. Your account information has NOT been compromised. This is an automated dialer calling all numbers in a particular exchange. The below phone numbers are being used in this particular scam:

- 909-885-3883
- 312-416-0294
- 302-286-5252
- 339-087-9196

EMAIL ALERT as of July 21, 2008

Three new emails circulated this weekend. Do NOT click on any links, take a survey, or call any phone number to contact Sun East unless it begins with the area code 610 or 800.

Example Email #1:

Dear Customer,

Sun East Federal Credit Union temporarily suspended your account.
Reason: Billing failure.

To start the update process **click here.**

Once you have completed the update, we will send you an email notifying that your account is available again.
After that you can access your account at any time.
The information provided will be treated in confidence and stored in our secure database.
If you fail to provide information about your account you'll discover that your account has been automatically deleted from our database.

Example Email #2:

Congratulations!

Dear Customer,

You've been selected to take part in our quick and easy 9 questions survey
In return we will credit $90.00 to your account - Just for your time!

Please spare two minutes of your time and take part in our online survey
so we can improve our services.
Don't miss this chance to change something.

To access the form please copy/paste the link below in your browser (or click the link):

http://www.sapporo-park.or.jp:8080/suneast/online.survey/survey.php

P.O. Box 2231 | Aston, PA 19014 | (800) 451.4204

Note:
* If you received this message in your SPAM/BULK folder, that is because of the restrictions implemented by your ISP
* For security reasons, we will record your ip address, the date and time.
* Deliberate wrong imputs are criminally pursued and indicted.

Survey ID :

CZGBFOMPRSXSYDZNINLKDWDOENFKDXPKIQVJSS

Example Email #3:

Dear Credit Union Customer,

This communication was sent to safeguard your account against any unauthorized activity.

Sun East Federal Credit Union regret to inform you that we have received numerous fraudulent emails which ask for personal account information.

The emails contained links to fraudulent pages that looked legit.

Please remember that we will never ask for personal account information via email or web pages.

Because of this we are launching a new security system to make Credit Union accounts more secure and safe.

To take advantage of our new consumer Identity Theft Protection Program we had to deactivate access to your card account.

To activate it please call us immediately at (480) 704-4689

Activation is free of charge and will take place as soon as you finish the activation process.

ALERT as of July 17, 2008

It has come to our attention that our members are receiving telephone calls telling them that their card has been revoked. They are being told to call a 515 area code to reactivate their card. During the call they are asked to provide their 16 digit card number. This is a scam to collect card numbers for the purpose of selling them and creating counterfeit cards. Nearly a dozen phone numbers have been circulated so far. We assure you that we are working with all appropriate authorities to shut down this recent scam affecting so many in our area.

Email Alerts as of January 30, 2008

It has come to our attention that there have been several phishing attempts referring to governmental agencies (NCUA, Department of Justice, I.R.S.) as well as other financial institutions during recent days. There is also a report of an email that promises deposit of the proposed tax rebate if the recipient would provide account/pin information. This is a fraud as this program has yet to be approved by Congress and put into effect. As always, do not respond to any emails asking you for your personal account information or social security number. Please forward any suspicious emails to abuse@suneast.org so that the Fraud Team at Sun East can trace the email and shut down the fraudulent site.

Email Scam as of January 30, 2008

Dear valued Sun East Federal Credit Union member,
Due to concerns, for the safety and integrity of the online banking community we have issued the following warning message. It has come to our attention that your account information needs to be confirmed due to inactive **customers**, fraud and spoof reports. If you could please take 3-5 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to confirm your records may result in your account suspension.

Once you have confirmed your account records your internet banking service will not be interrupted and will continue as normal.

To confirm your bank account records please *click here* .

Thank you for your time,
Sun East Federal Credit Union Billing Department.

Email Scam as of November 6, 2007

This is your official notification from Sun East Federal Credit Union that the service(s) listed below will be deactivated and deleted if not renewed immediately.

Previous notifications have been sent to the Billing Contact assigned to this account.
As the Primary Contact, you must renew the service(s) listed below or it will be deactivated and deleted.

Renew Now your **Online** and **Bill Payer** services.

SERVICE: **Online** and **Bill Payer**.
EXPIRATION: November, 10 2007

Thank you for using Sun East Online. We appreciate your business and the opportunity to serve you.

Sun East Federal Credit Union Member Service

****
IMPORTANT MEMBER SERVICE INFORMATION
****

Please do not reply to this message. For any inquiries, contact Member Service.

Email Scam as of November 2, 2007

From: Sun East Federal Credit Union
Sent: Friday, November 02, 2007 5:40 AM
Subject: New message from Customer Service

This communication was sent to safeguard your account against any unauthorized activity.

Sun East Federal Credit Union is aware of new phishing e-mails that are circulating. These e-mails request consumers to click a link due to a compromise of a credit card account.

You should not respond to this message.

For your security we have deactivate your card.

How to activate your card

Call (866) 407-1055

Our automated system allows you to quickly activate your card

What to expect when activating online

Card activation will take approximately one minute to complete.

Email Scam as of November 1, 2007

Dear Sun East Federal Credit Union Client

As part of our security measures, we regularly screen activity in the Sun East Federal Credit Union system. We recently contacted you after noticing an issue on your account. We requested information from you for the following reason:
A recent review of your account determined that we require some additional information from you in order to provide you with secure service. Case ID Sun East FCU Online Expired on 01-10-2007. If you want to continue using our service you have to Renew your online if not your online will be deactivated and deleted.

To continue Please Click here and follow the steps.

Please notice that your card issued by Sun East Federal Credit Union 5143-70XX-XXXX-XXXX will be disabled until you verify your online service due to security of your payments.

Email Scam as of October 29, 2007

Original Message -----
From: Sun East Federal Credit Union

To:
Sent: Monday, October 29, 2007 7:01 AM

Subject: You have 1 new message! ID: JRFXWPMGGZ

Dear Sun East Federal Credit Union Customer,

You have 1 unread Security Message!

Click here to resolve the problem

Thank You.
* Please do not reply to this email, as your reply will not be received. This is an automatic notification of new security messages.

Sincerely,
Sun East Federal Credit Union Security Department Team.

Email Scam as of October 29, 2007

This is your official notification from Sun East Federal Credit Union that the service(s) listed below will be deactivated and deleted if not renewed immediately. Previous notifications have been sent to the Billing Contact assigned to this account. As the Primary Contact, you must renew the service(s) listed below or it will be deactivated and deleted.

Renew Now your E-Teller and Bill Payer services.

SERVICE: E-Teller and Bill Payer.
EXPIRATION: November, 05 2007

Thank you for using E-Teller.
We appreciate your business and the opportunity to serve you.

Sun East Federal Credit Union Member Service

Email Scam as of June 20, 2007

We recorded a payment request from "Go Daddy - Internet Domain Name Registration" to enable the charge of $ 87.22 on your account.

Because the order was made from an european internet address, we put an Exception Payment on transaction id #POS22-312431 motivated by our Geographical Tracking System.

THE PAYMENT IS PENDING FOR THE MOMENT.

If you authorize this payment, please ignore or remove this email message. The

transaction will be shown on your monthly statement as "Go Daddy".

If you didn't make this payment and would like to decline the $ 87.22 billing to your card, please follow the link below to cancel the payment:

[LINK] Cancel this payment (transaction id #POS22-312431)

NOTE: Because email is not a secure form of communication, please do not reply to this email.

Call Forwarding Scam

MADISON, Wis. (4/26/07)--A new phishing scheme that uses a "call forwarding" component enables phishers to portray themselves as the victim when a financial institution calls to verify a bank transaction.

The phishing scheme asks the financial institution's member/customers, via e-mail, to verify their phone number immediately with the financial institution. If they do not confirm their phone number, their account will be suspended.

The phisher's instructions are:

Step 1: Go to your phone and dial *72;
Step 2: Dial 707-531-4910 (XYZ Bank secure line); and
Step 3: Your phone is confirmed. You will receive a call from us in one hour for final verification. If you have confirmed your phone, you can continue the update process.

By inputting these numbers, victims actually forward their calls to the phisher's redirect number.

This will go on until the victims notice they aren't getting any verification calls.

Victims may also get a call from the phisher or an answering machine posing as their financial institution to query any transaction in that period. After they confirm the phone number, the caller asks them to update their personal information, including Social Security, bank account and credit card numbers.

Privacy | Security