

****URGENT NOTICE TO MEMBERS****

You may have heard in the news about the recent hacker attacks or security breaches in which criminals are able to obtain credit and debit card information on large numbers of people. Unfortunately, credit and debit card numbers are prime targets of criminals, and these breaches have been fairly common in recent months. Such breaches are troublesome, since the criminals' intent is to obtain card data for the purpose of creating counterfeit cards and making fraudulent transactions on the cardholder account. Rest assured that there has been no breach of any Pocatello Teachers Federal Credit Union system. We go to great lengths to make sure that our security measures are always maintained under very tight controls. Regrettably, our cardholders can still be affected by these situations when third-party systems are breached. Here are some questions we are frequently asked about such situations:

FAQ's:

Q: How will I know if my account has been compromised?

A: Members of our staff will contact you. We will attempt to contact you by mail, telephone, or possibly e-mail. Remember that Pocatello Teachers Federal Credit Union employees will never ask your account number, PIN number, or other account information over the phone or by e-mail.

Q: What happens if my account has been compromised?

A: We will most likely need to block your credit or debit card and re-issue a new card number to you.

Q: Which merchant was compromised?

A: TJX Companies, includes T.J. Maxx, Marshalls, HomeGoods, Bob's Stores, and A.J. Wright in the U.S., Winners and HomeSense in Canada, and T.K. Maxx in Europe.

Q: How long will it take to get my new card?

A: Debit or Credit cards will take 7 – 10 days, and they will be mailed to your home.

Q: What if I can't wait that long for a replacement credit card?

A: In case of emergency, we can expedite the replacement cards, and usually have them to you in about 48 hours.

Q: Has my identity been compromised? Should I worry about identity theft?

A: Most likely not. The data contained in compromised databases will usually be limited to card information. Blocking the card account in question and re-issuing a new number should solve the problem, but it is always a good idea to check your credit report and exercise caution where your identity is concerned.

Q: What happens if I have fraudulent transactions on my account?

A: Contact the credit union immediately to dispute any fraudulent transactions. We will take action quickly to prevent any additional fraud, and to remove the fraudulent transactions from your account. Under normal circumstances, our goal is to act quickly and proactively to prevent fraud from ever occurring.

Q: I have heard that criminals often try to steal card and personal information by sending e-mails. Is this situation related to e-mails or the internet?

A. The e-mails you describe are called "phishing" e-mails, and are designed to get you to key personal or card information into bogus websites which are disguised as legitimate sites. These e-mails often mimic sites from financial institutions or from popular internet sites. Remember that no legitimate financial institution or business will ask you to "update" or "activate" your account via a link in an e-mail. You should **never** respond to e-mails of this type. If you receive suspicious e-mail, you can forward them to ptfcredit@qwest.net. Subject: Fraudulent email.

Q: How can I prevent this from happening?

A: This situation occurred when criminals hacked into a merchant database. It was not due to any action or inaction on your part. When these situations arise, rest assured that we will contact you and take appropriate action.

01/30/2007