

## Frequently Asked Questions

### Compromised Debit Cards

#### **What is a ‘compromised’ Debit Card?**

A card is considered ‘compromised’ when it is at risk of being used in a fraudulent manner. This can happen as a result of the theft of data stored in a computer, unauthorized computer network access, or of any other suspicious event. Card information can also be stolen when shopping at a store or when data is sent electronically when making an online payment

#### **What does PSFCU do to notify members that their card information has been obtained by unauthorized persons?**

The Polish & Slavic Federal Credit Union (PSFCU) treats all such events with the utmost caution. So much so, that we require all compromised cards, regarded as high-risk, be canceled immediately. We replace them with a new card at no cost to the cardholder. As a rule, we attempt to contact the cardholders by phone or by mail to inform them about the situation.

**Does this mean that unauthorized transactions have been posted to my account? The fact that a card is considered ‘compromised’ does not** mean fraudulent activity is present. In fact, this happens very rarely and of all the compromised card numbers we receive, very few of those have unauthorized transactions posted.

#### **How can I avoid such situations?**

We advise you to monitor your monthly account statement closely and systematically. As an added advantage, our Internet Banking allows you a constant access to view your account transactions.

#### **Do all financial institutions block compromised cards and issue new ones after being informed that card numbers have been disclosed to unauthorized persons?**

No, there is no such requirement. Some institutions don’t even inform their clients that they have received such information. They pass all responsibility for discovering fraud onto their clients. Conversely, PSFCU wants to protect our members from unauthorized use of stolen card numbers. This protects them against thieves who could use these numbers in the future, even months or years later. To evade such situations, we void these cards and issue new ones as soon as we receive information that the card numbers have been compromised.

#### **What should I do if I notice fraud on my Debit Card account?**

If the card has not yet been blocked, immediately call PSFCU at 1-855.PSFCU.4U (1.855.773.2848). After business hours, please call 800-472-3272.

**What happens when a unauthorized transaction on my account clears and a lack of funds prevents me from fulfilling my financial obligations?**

In the majority of cases, PSFCU will issue a temporary credit to member account which can be used while the investigation is in progress. We emphasize, however, that any fraud has to be reported to the PSFCU as soon as possible.

**How soon after my card is canceled will I receive a replacement?**

In the majority of cases, cards are received within two weeks from the order date. A new PIN number will be delivered three to four days after you receive your card.

**What should I do if I do not receive a replacement card in time?**

Please contact us at 1-855.PSFCU.4U (1.855.773.2848). After checking the shipment status, we will be able to provide you with further assistance.

**What should I do after I receive a new card?**

Upon receipt of your new card we ask that you destroy your old one. You may then proceed to activate the new card by following the attached instructions.

**Will my PIN number change when I receive a new card?**

Yes. You will receive a new PIN number consisting of randomly selected digits, which will differ from the compromised information. To change the PIN number issued by the card processor to one at your preference, please visit a Member Services Representative at any PSFCU branch.

**Is there a fee for a replacement Debit Card?**

No, PSFCU does not charge any fees for replacing a Debit Card.

**Can I avoid canceling my card even though its number has been compromised?**

Every report that indicates possible fraud constitutes a serious threat to the funds deposited into your account. If the old card is not canceled, your account will remain at risk of unauthorized activity which could take place a days, weeks, months or even years later. Moreover, recovering lost funds can be a long and arduous process. While the amount of cases with unauthorized use is low, a risk of such activity will remain present until the card is replaced. To limit any losses and inconveniences arising from potential fraud, PSFCU requires that all compromised cards be replaced immediately.

**What should I do if I have existing authorized automatic payments scheduled with various merchants?**

Notify the company collecting the automatic payments immediately after receipt of a replacement card. You will have to change the card number and its expiration date. In some cases, you will be able to change this information on the company's website while other's will require a written notification. Consequently, please check the requirements directly with the company collecting such payments.

**Does theft of one Debit Card number put another card, tied to the same account, at risk?**

It depends. The fact that each card has a unique number reduces the risk of unauthorized use if only one number has been stolen. As a result, PSFCU takes measures to prevent the unauthorized use of card information. As a result, if data on an additional card has been stolen as well, PSFCU will take the same steps for both cards on this account.

**Is stealing card information the same as identity theft?**

Information coded on the Debit Card relates solely to the card itself such as the number and the expiration date. Personal data, such as the cardholder's Social Security number, driver's license number, address, or date of birth are never recorded on the card.

**Can I protect myself against Debit Card information theft in the future?**

Unfortunately, at this time there is no method of completely shielding client's from had information stolen from retail databases or payment clearing houses. The risk can only be significantly reduced by avoiding the use of your Debit Card online.

**What steps can I undertake in the future to protect my card against potential fraud?**

- Always remember where you store your card. If you ever lose it, contact PSFCU immediately. The card will be immediately canceled to prevent it from unauthorized use. (After business hours, please call 800- 472-3272)
- Under no circumstances should you write your PIN number on your card.
- Never carry a written PIN number with you.
- Check your monthly statements thoroughly and systematically, immediately after you receive them.
- We recommend using our Internet Banking, which allows you a round-the-clock access to your account. You can also check you transactions by phone by contacting our Call Center at 1-855.PSFCU.4U (1.855.773.2848).
- Should you notice any inconsistency, contact us immediately.

**What should I do if I notice an unauthorized transaction that has been posted to my account?**

In order to be eligible for a refund of your money, you need to take the following measures:

- Please contact the company which received payment from your account to inform them that the transaction was not authorized by you and constitutes fraud resulting from stolen information.
- Immediately report any unauthorized transaction to PSFCU at 1-855.PSFCU.4U (1.855.773.2848). Proceed to fill out an Affidavit of Fraud which will be submitted to the Card Servicing Department as soon as possible. When filling out this form, please provide information about the company which received the payment, the date of the unauthorized transaction, any responses from the company which received the payment after the fraud has been reported, and the amount of the fraudulent transaction together with any other important details which may aid the investigation.

