

## **Mt. Washington Bank Frequently Asked Questions on Compromised Cards**

You may have read in the paper or seen it in the news, there has been a lot of media attention in relation to credit card and/or debit card information being compromised. In an effort to educate our customers about compromises and how Mt. Washington Bank handles compromise notifications, we have put together some helpful information and answered some of your most commonly asked questions. For in depth information about the various fraud scams and what you can do to protect yourself, visit our Protect Yourself Against Fraud section on our website.

### **What is a compromised card?**

A compromised card means that information (for example card number, name, and expiration date) may have been obtained by an unauthorized source. A compromised card is a card that is at risk of being used fraudulently. Cards may be compromised due to computer theft, unauthorized network intrusion, or any type of suspicious activity

### **How does Mt. Washington Bank react to compromise notifications?**

Mt. Washington Bank takes every compromise seriously and requires issuance of new cards for affected customer. Customers will receive written notification if their card data has been compromised. The notification will provide detailed information on obtaining a replacement card.

### **Does this mean I have fraud on my account?**

Not necessarily. A compromised card letter does not mean any fraudulent activity occurred on your account. In fact, among the list of card numbers we periodically receive, only a few have been affected by fraud. Take the opportunity to review your monthly statement(s). Remember to review your daily transactions using Online Banking.

### **What do I need to do if I discover fraud on my account?**

If your card has not been blocked already, call the bank immediately. For Debit Card transactions, you will need to complete our Cardholder Dispute Form with Affidavit. If you have questions about the form, please call our Ultimate Service Department at 617-268-8880.

### **How long will it take to receive my replacement card?**

Most cards are received within two weeks from the date of order. The new PIN is delivered one to two days after that.

### **What happens if I do not receive my card by this time?**

Please contact our Ultimate service Department at 617-268-8880 so we can check on this immediately.

### **What do I do when I receive my new ATM or Debit Card?**

Cut up the old compromised card and you must activate the new card received. The compromised card will be blocked from further activity 30 days after the date on your notification letter.

**Will my PIN number change along with my card number?**

Yes, the new card number will have a new randomly generated PIN number. This is done in order to protect your privacy and ensure that your personal PIN number was not included in the compromise.

**Is there a charge for the new card?**

As a courtesy to our customers, under these circumstances, we do not charge the normal \$5.00 replacement fee.

**What if I do not want to have my compromised card blocked?**

Compromises are serious. Fraudulent activity may occur if the card is not blocked. The fraud dispute process can be more inconvenient to customers than simply having a card replaced. While, many customers do not experience fraud when a compromise is reported, the risk exposure still exists if the cards are not blocked and replaced. To protect our customers, minimize inconvenience and losses, Mt. Washington Bank requires compromised cards to be replaced.

**What if I have preauthorized debits made to my compromised card number?**

You should contact the merchant immediately upon receipt of your replacement card and provide them with the new card number and expiration date. This process may be as simple as logging into the corresponding merchant's site and updating the information yourself. If this is not the case, you may need to write to let them know of a card number change.

**There are other authorized users on my Debit Card account. Does this affect their card(s) too?**

Debit cards each have a separate number. Therefore, if one card is compromised, that doesn't always mean the authorized user's card is compromised as well.

**Can this information be used to steal my identity?**

The information encoded on the compromised card pertains strictly to the card, potentially including the name, card number and expiration date. Confidential information such as Social Security Numbers, driver's license numbers, addresses and dates of birth are not stored on the card.

**What can I do to keep this from recurring?**

Unfortunately, we have no way of stopping criminals from hacking into databases of merchants. While the possibility of a card being used fraudulently is low, we recognize the aggravation customers face in acquiring a replacement card or to have fraudulent activity removed from their account.

**Is there anything I can do to insure that fraud doesn't occur on my card?**

Always know where your card is, and if you misplace it, call the bank immediately so we can block the card from use. Never write your PIN on the card or carry the written PIN with you. Use online Banking to watch your account activity and call 617-268-8880 if you see anything suspicious.