

Memorandum

To: All Cumberland Security Bank customers
From: Mike Simpson, CEO
Date: March 4, 2009
Re: Notification of Card E-mail Scam

Cumberland Security Bank wants to make you aware of an e-mail-based card scam where consumers have been falsely notified that their Visa cards may have been compromised due to fraudulent activity.

The e-mail provides official-looking information about Visa's commitment to fighting fraud, along with a false "Case ID Number" and a directive for cardholders to verify their identity via the Web in order to continue using online services. This e-mail is a fraudulent attempt to obtain sensitive cardholder information. Here is a sample of an actual fraudulent e-mail that was sent.

Dear Visa Cardholder,

Continuous Monitoring is an integral part of Visa's multiple layers of security. In addition to other fraud monitoring tools, we can often spot fraud based upon transactions on the card that are outside of cardholders typical purchasing pattern.

This allows us to spot fraudulent activity as quickly as possible and acts as an early-warning system to identify fraudulent activity.

During a recent checkout we detected suspicious activity and your Visa card may have been compromised. Fraudulent activity made it necessary to limit your card for online services. Your Case ID Number is: **DD7Q8QQ9EDR7**

Conform to our security requirements and in order to continue online services with your card, we must validate your identity.

[Please click here to verify your identity.](#)

Visa takes online security very seriously so that you can shop safely on the Internet. As part of our commitment to fighting fraud we have the right to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, or violations of the terms and conditions for using Visa.

Sincerely,
Visa Customer Service.

© Copyright 2001-2009, Visa All Rights Reserved.

Cumberland Security Bank reminds you that no financial institution will request account, card or PIN information over the phone or via e-mail. Any time that information is requested, you should alert your financial institution of a potential scam. If you believe you may have already been a victim of fraudulent requests for information, you may call us at 606-679-9361.