



## IMPORTANT NOTICE TO CUSTOMERS

We have recently received a large list of Oceanside Bank check cards potentially impacted by the recent Heartland data compromise. This compromise took place during the third and fourth quarters of 2008, and has involved millions of cards throughout the nation. We believe that those perpetrating this incident may have accessed your card account number and the secret code on the magnetic stripe that prevents counterfeit cards. It's important to note, though, that although your information may have been compromised, it does not necessarily mean fraud has occurred on your account. Also, there wasn't any personally identifying information stolen such as Social Security numbers, so we believe that the risk of identity theft is reduced.

Because we are committed to ensuring your accounts are safe, we have reissued your card to protect you from fraud. Additionally, all consumer Visa credit and debit cards are protected with Visa's Zero Liability policy in the rare event fraud does occur, which means you pay nothing for fraudulent activity on your account. We urge all of our customers to watch their check card transactions closely, and contact us at 904-247-9494 if you suspect unauthorized activity on your account.

### FAQ Regarding Recent Card Security Breach

**What is Heartland and what does it have to do with the Oceanside Bank check card?**

Heartland is a payment processing service that retailers use to process their credit and debit transactions from customers. It's a back end process that is on the retailer side, not on the side of the financial institution.

**What should I know about security and card fraud?**

The most important thing to remember is that you should never give out personal or account information to someone who calls you.

If you have questions about your check card, always call Oceanside Bank's main phone number at 904-247-9494. This will help ensure you're really speaking to the right person or company.

Also, remember that attempts to get your personal information can come in any form. Do not respond to phone calls, emails, text messages or any other form of communication asking you to provide personal or account information.

**I recently noticed fraud on my account. Is this fraud related to the recent incident?**

It is unclear whether this fraud is related to the Heartland Payment Systems incident. It is important to know that regardless of where the fraud occurred, you are protected by Visa's Zero Liability policy.

**How did this happen?**

When your card is swiped at a merchant or you enter your number into the computer when buying online, the information is transmitted to third parties that process that information so your card-issuing bank or credit union can accept your transaction. A criminal may have gained access to your card information through one of the entities involved with processing your transaction, including the merchant. While fraud resulting from data compromises is rare, it's important to understand that you're protected with Visa's Zero Liability policy.

**Has the security breach been fixed?**

Yes, the affected merchant (or processor) is working to ensure no further information is exposed.

**What are the chances that I will become a victim of identity theft as a result of this incident?**

It is important to know that there wasn't any personally identifying information stolen such as Social Security numbers. In fact, fraud rarely occurs on accounts compromised during a data breach. It's always a good idea to regularly check your credit report for incorrect information. Also, you're entitled to one free copy of your credit report every year at [www.annualcreditreport.com](http://www.annualcreditreport.com) or by calling 1-877-322-8228.

**What is Oceanside Bank doing to protect my personal account information, especially in this case?**

Oceanside Bank and Visa are working closely together to catch any fraudulent behavior and protect your account. Oceanside Bank offers consumers multiple layers of security protection against fraud, including Visa's Zero Liability policy, the cardholders' ultimate protection. With Zero Liability, consumers are not responsible for any unauthorized purchases made with their Visa cards. Visa recently announced a breakthrough, patent-pending, antifraud technology called Advanced Authorization. This technology instantaneously analyzes every Visa credit and check card transaction's potential for fraud, including whether it was part of a reported data compromise. It can also pinpoint coordinated attacks on multiple accounts in real time. Advanced Authorization is being applied to every Visa credit and check card purchase today.

**What can I do to ensure this doesn't happen to me again?**

While we employ the latest systems and technology to monitor and prevent card fraud and many merchants also take the necessary precautions to protect your card information, there are some practical steps you can take to help protect your card information:

- 1) Shop with merchants you know. If a deal seems too good to be true, it probably is.
- 2) Check your account statement promptly and immediately report any transactions that you don't recognize.
- 3) Destroy all receipts before discarding them since some of them may have your card number reprinted on them.
- 4) Guard your card – don't use it as collateral or give out your card number to someone calling on the phone, unless you initiated the call for a purchase.
- 5) Check your credit report at least annually to ensure its accuracy.
- 6) Never write down your PIN. Memorize it as soon as you get it.
- 7) Do not disclose your PIN to anyone. No one from any bank, the police or a merchant should ever ask for your PIN.
- 8) Beware of phishing emails. These are emails that appear to be from your bank or online merchant asking for account information. Do not reply to them or click on any links. Visa, your bank or any other legitimate online merchant will ever ask for your PIN or other personal information via email.
- 9) At an ATM or PIN pad, enter your PIN discreetly, shielding the key pad with your hand.

**What should I do if I experience fraud on my account?**

- 1) Review your monthly statement to spot any unauthorized purchases. You can also monitor your account activity online at any time with Online Banking at [www.OceansideBank.com](http://www.OceansideBank.com).
- 2) Please let us know immediately if you see unauthorized purchases. You may speak to an Oceanside Bank Check Card Specialist at **904-247-9494** from 8:30 a.m. to 5 p.m., Monday through Friday. During non-business hours, please report lost or stolen cards to 1-800-554-8969.
- 3) You should also contact the three credit reporting agencies to notify them of any suspected fraud or identity theft:

<b>Equifax®</b> 800-525-6285 <a href="http://www.equifax.com">www.equifax.com</a>	<b>Experian®</b> 888-397-3742 <a href="http://www.experian.com">www.experian.com</a>	<b>TransUnion®</b> 800-680-7289 <a href="http://www.transunion.com">www.transunion.com</a>
---	--	--