

Security Breach Tips

Q: There are reports of a data breach. How is this affecting my iAB ATM/debit card?

A: Unauthorized access to a retailer's system, results in the compromise of credit and debit card information. Although certain card account data may be compromised, that does not mean data related to your account was taken, or that fraud has occurred on your account. Please be assured that we actively monitor the activity on your account to protect you from fraud. You will be contacted if we see any activity that requires you to take action.

In addition, please be sure to review your monthly and/or online statement carefully and call us immediately if you see any suspicious activity. It's also important to note that all 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 unauthorized purchases on your account.

Q: If I become a victim of identity theft, how will you help to restore my good name?

A: In the unlikely event you become a victim of identity theft, the consumer network group, Call for Action, provides consumers with free and confidential assistance from trained counselors. The toll-free telephone hotline can be reached at 1(866) ID-Hotline for assistance with identity theft.

Q: What is iAB doing to protect my personal account information?

A: Working with Visa, iAB Financial Bank offers consumers multiple layers of security protection against fraud, including Visa's Zero Liability policy. With Zero Liability, consumers are not responsible for any unauthorized purchases made on their Visa card.

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

A: While we employ the latest systems and technology to monitor and prevent card fraud and 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:

- Shop with merchants you know. If a deal seems too good to be true, it probably is.
- Check your account statement promptly and immediately report any transactions that you don't recognize.
- Guard your cards – don't use it as collateral or give out your card number to someone calling on the phone, unless you initiated the call.
- Check your credit report at least annually to ensure its accuracy. Contact any of the three credit reporting agencies.
Equifax – 800-685-1111 Experian – 888-397-3742 TransUnion – 800-916-8800

Q: What should I do if I experience fraud on my account?

A: Please monitor your account – both your monthly statement and online – and let us know immediately if you see unauthorized purchases. You should contact us immediately at the numbers listed at the end of this document.

Q: Are there any other tips you can provide to reduce my chances of card fraud?

A: Yes. There are several actions you can take to protect your personal information.

DO . . .

- Shred all personal and financial information such as bills, bank statements, ATM receipts and credit card offers before you discard them.
- Keep your personal documentation (i.e., birth certificate, Social Security card, etc.) and your bank and credit card records in a secure place.
- Call the post office immediately if you are not receiving your mail. To get the personal information needed to use your identity, a thief can forge your signature and have your mail forwarded.
- Be aware of your surroundings when entering your Personal Identification Number (PIN) at an ATM or merchant location.
- Limit the number of credit cards and other personal information that you carry in your wallet or purse.
- Report lost or stolen credit cards immediately.
- Cancel all inactive credit card accounts. Even when not being used, these accounts appear on your credit report, which is accessible to thieves. If you have applied for a credit card and have not received the card in a timely manner, immediately notify the card provider.
- Closely monitor the expiration dates on your credit cards. Contact the credit issuer if the replacement card is not received prior to your credit card's expiration date.
- Sign all new credit cards upon receipt.
- Review your credit reports annually.
- Use passwords on your credit cards, bank accounts, and phone cards. Avoid using the obvious passwords – such as your mother's maiden name, your birth date, and the last four digits of your Social Security or phone number.
- Match your credit card receipts against monthly bills to make sure there are no unauthorized charges.

DON'T . . .

- Volunteer any personal information when you use your card.
- Give your Social Security number, card number, or any bank account details over the phone unless you have initiated the call and know that the business that you are dealing with is reputable.
- Leave receipts at ATMs, bank counters, or unattended gasoline pumps.
- Leave envelopes containing your credit card payments or checks in your home mailbox for postal carrier pickup.
- Record your Social Security number or passwords on paper and store them in your wallet or purse. Memorize your numbers and/or passwords.
- Disclose bank account numbers, debit/credit card account numbers, and other personal financial data on any web site or online service location, unless you receive a secured authentication key from iAB.

Helpful Numbers

If you believe you are a victim of fraudulent activity on your iAB debit or credit card, immediately contact iAB during regular business hours at (260) IAB-BANK (422-2265). After business hours, call: ATM/debit card services: 800-791-2525
Credit card services: 800-883-0131

