
ATM/VISA DEBIT CARD FRAUD DETECTION

Your financial security is important to Sharon Savings Bank. ATM/Visa Debit Card holders of Sharon Savings Bank are protected from ATM/Debit Card fraud by a fraud detection/prevention system known as the FIS Fraud Alert Management System. This system is designed to recognize potentially fraudulent debit card transactions based on cardholders behavior, transactional data, credit/debit modeling techniques and fraud analytical strategies.

This system analyzes and recognizes specific fraud patterns. If a transaction triggers an alert, the FIS Fraud Call center will initiate a call to the customer identifying themselves as “Card Security”.

The customer is still responsible for reviewing their monthly statement each month. If an unauthorized transaction appears on your statement you should contact the FIS Alert Management Team immediacy to report the activity. They can be reached **24/7** at **1-866-537-2830**.

In addition, customers can also report their card lost or stolen and have the FIS Call Center hot card their card immediately.

➤ **What should I expect if there is possible fraudulent activity on my ATM/Visa Debit card?**

You will receive a phone call to the phone number associated with your account from the FIS Alert Management team member.

➤ **How will the FIS Alert Management team member identify themselves?**

When you answer the call, they will identify themselves as “Card Security”. The team member will request to speak to the owner of the card and ask them to identify themselves by providing the last four digits of the accounts owners’ social security number.

Please note: The FIS Alert Management team **will never** ask for a customer’s entire social security number.

➤ **Why do I have to verify my identity with FIS Fraud Alert Management?**

For security purposes, the FIS Fraud Alert Management team will always verify contact primary cardholder of the account. You will be only asked to verify the *last four numbers* of their social security number.

For card holders who choose not to verify any type of personal information, the FIS Fraud Management team will request that you contact Sharon Savings Bank directly for further information.

➤ **What happens if I receive a call from the FIS Fraud Alert Management System? Will my card be blocked from use?**

If you verify the transaction(s) as authorized, your card will not be blocked. You will be able to use your card as normal.

If you verify the transactions(s) are *not authorized*, your card will be blocked.

➤ **What do I do after I verify a fraudulent transaction?**

Your ATM/Visa Debit card will be hot carded. A claims process for disputed transactions will be put in place. A letter will be sent to you via USPS. A copy of this letter needs to be brought into the bank to formally start the investigation. If you do not want to wait for the letter, come into any one of our offices and obtain an ATM Cardholder Dispute form or Visa Fraud form, depending on the type of card you have. Once the bank receives a signed affidavit, the investigation will begin.

A new ATM/Visa Debit card will not be issued automatically. The customer must come into the branch and complete a new application.

➤ **What should I do if I am going to be traveling?**

Transactions outside your normal pattern can create fraud alerts.

Be fore traveling, contract your local Sharon Savings Bank branch and let them know you will be traveling out of the area. A special temporary code can be added to your account while you are away to avoid unnecessary fraud alerts.

➤ **What can I do to help FIS Fraud Alert Management monitor my account and to protect my account from fraud?**

Keep your contact phone number current with the bank so you can easily be reached.

Follow safe practices with your Sharon Savings Bank ATM/Visa Debit Card;

- Treat your card like cash. Keep it in a safe place
- Do not disclose your personal identification number (PIN) to anyone.
- Never disclose card information in response to an unsolicited email request.
- Report a lost or stolen card at once.
- Carefully review your account statements.
- Block the view of others when entering your PIN information at POS or ATM terminal.
- Make sure you receive a receipt after completing a transaction either a point of sale or ATM terminal.