



Fraud Protection

Keeping your personal information secure

HSA Bank is dedicated to protecting your personal and financial information - it's a top priority here. We adhere to the Federal Financial Institutions Examination Council (FFIEC) requirements including strong authentication, fraud detection, and general layered security.



Fraud monitoring:

- HSA Bank uses a variety of fraud-monitoring tools to review how and where debit cards are being used. This enables us to identify abnormal patterns and to block potentially fraudulent transactions. We continually review and update our monitoring program to address activity trends.
- Should HSA Bank discover abnormal activity, the account will be restricted and the member will be notified by an experienced customer service representative who will walk them through next steps.

Blocking high-risk transactions:

- HSA Bank proactively limits the use of debit cards to qualified medical expenses and only at medically-related merchants (the debit card won't work at a gas station, restaurant, or rental car location, etc.).
- Debit cards are also limited to use within the United States and US foreign territories to prevent offshore fraud.
- Daily limits are set on the cards for ATM withdrawals as well as PIN and signature-based transactions.
- Cards are restricted after several invalid PIN attempts have been made. Cards are also restricted after exceeding a maximum number of attempted/denied transactions per day.

We've got you covered:

- In the event the card or card number is lost, stolen, or used without the member's authorization, the member must notify HSA Bank immediately. Members may not be liable for any unauthorized transactions. Members should refer to their Deposit Account Agreement and Disclosures for complete details on the protections provided to members regarding unauthorized transactions.

Credit:

- Once HSA Bank is properly notified of an unauthorized transaction, the member will be credited promptly while we investigate the unauthorized transaction dispute. Final credit to the HSA is subject to verification.

Easy access to balance information:

- Members have the ability to review account balances, recent purchases, and ATM transactions online to quickly identify any potential fraudulent activity.
- Members can also access our automated phone system 24/7 for balance inquiries.
- Members can elect to receive email notifications when various transactions occur or when the balance reaches a pre-specified amount.

To report unauthorized transactions:

- Call our Client Assistance Center immediately at 800-357-6246 and an experienced customer service representative will assist you immediately to protect your account and give you peace of mind.

Non-card-specific fraud prevention features:

- Members can use our online banking system to conduct transactions. Online banking users must set up security questions for dual-factor authentication to access online transaction functionality. Any external banking accounts that are linked to the health account also undergo a validation process prior to activation.
- Last login date/time and access mechanism is presented in the online banking screens which allows the member to see the last time their online account was accessed.

Tips for Protecting Yourself from Fraud:

- NEVER respond to an email, phone call, or text message that asks for your personal or account information.
- NEVER reveal your username or password to anyone.
- Periodically change your password.
- Don't leave your computer or mobile device unattended when logged into your account.
- Review account statements regularly and report unauthorized activity.

For assistance, please contact the Client Assistance Center



800-357-6246

www.hsabank.com | 605 N. 8th Street, Ste. 320, Sheboygan, WI 53081

