Fraud protection

Keeping your personal information secure

HSA Bank is dedicated to protecting your personal and financial information. 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 you'll be notified by an experienced customer service representative who will walk you through next steps.

Blocking high-risk transactions

HSA Bank proactively limits the use of debit cards to IRS-qualified healthcare expenses and only at healthcare-related merchants (the debit card won't work at a gas station, restaurant or rental car location, etc.).

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 your authorization, you must notify HSA Bank immediately.

You may not be liable for any unauthorized transactions.

You should refer to your Health Savings Account Custodial Agreement for complete details on the protections provided regarding unauthorized transactions.

Credit

Once HSA Bank is properly notified of an unauthorized transaction, you'll be credited promptly while we investigate the unauthorized transaction dispute.

Final credit to the HSA is subject to verification.

Easy access to balance information

Review account balances, recent purchases and ATM transactions online to quickly identify any potential fraudulent activity.

Access our automated phone system 24/7 for balance inquiries.

Elect to receive email notifications when various transactions occur or when the balance reaches a prespecified amount.

Non-card-specific fraud prevention features:

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 bank accounts that are linked to the health account also undergo a validation process prior to activation.

To report unauthorized transactions:

Call the number on the back of your debit card immediately. An experienced customer service representative will assist you in protecting your account.

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 use the same password for multiple websites.
- Don't leave your computer or mobile device unattended when logged into your account.
- Review account statements regularly and report unauthorized activity.
- Set up alerts in the Customer Website under Settings to notify you of activity on your HSA.

Call the number on the back of your Cigna Healthcare® ID card

hsabank™ cigna healthcare

Fraud_Protection_Cigna_100325