bankSA

What's next if you've reported a Card scam or fraud case?

This leaflet contains important steps and information to help you navigate our fraud and scam process and stay protected in the future.

My case number

Now that you have alerted our Fraud and Scams team about your recent activity, here's what will happen next.

Step 1: Things we will do.

- We'll attempt to stop any transactions, where we can intervene.
- We'll cancel and replace any compromised cards.
- You can locate your Digital Card in the BankSA App. For help to access visit ***banksa.com.au/digitalcard***
- We'll advise you of our timeframes (which may vary from case to case).
- We'll send you an email or SMS to confirm your case has been created.

Step 2: Things you can do.

- Contact us immediately if you identify further unusual transactions.
- Report any financial loss to the Australian Signals Directorate (ASD) Cyber team at ***cyber.gov.au/report***

IDCARE:

- Engage IDCARE for free, confidential support at ***idcare.org***
- BankSA has partnered with IDCARE, Australia and New Zealand's National Identity & Cyber Support Service to provide guidance to people who have been targeted by fraud, scams, identity theft or compromise.

- IDCARE can help create a tailored response plan for your financial accounts and any other personal details, mobile phone or email accounts, utilities and social media accounts.

Step 3: During the investigation.

- Want an update on your case? Call us on ***1300 301 217*** or via the App
- We'll contact the merchant with all attempts made to recover your money, where possible.
- We'll investigate if your activity qualifies for our BankSA Fraud Money Back Guarantee. If you're eligible for a refund, we'll notify you and credit the funds back to the account debited. For more information visit ***banksa.com.au/secure***
- If your investigation is deemed a scam where we can recover funds from the merchant, it will be processed back to your account.

FAQs

Please find below answers to some of our most common customer questions.

1. How did my card get compromised?

- A common way is through online data breaches from merchants and payment providers. Your card number can also be at risk from phishing, where you might enter your card details on a fake website. Additionally, criminals use force to guess your card credentials, such as BIN (Bank Identification Number) attacks or card guessing.
- In a BIN attack, criminals use the first six digits of your card number (the BIN) to algorithmically generate the remaining numbers. They then test these combinations to find a valid card number.

2. Will I receive a new card number?

- Yes, you will receive a new card with a new card number, expiry date and CVV. This will be linked to the same account number as before. Your Digital Card will also be available while you wait for your new card.

3. How long will the investigation take?

- Normal cases take 21 days. More complex cases can take up to 45 days.

4. Do you refund the money straight away?

- If eligible the money gets refunded to your card, so you are not out of pocket. The bank then attempts to recover funds through the chargeback process.

5. How can I stop this from happening again?

- You can avoid being impacted by being careful where you share your card details online. Avoid saving your card details to online stores and use the Digital Card (see below) to prevent reuse of your details.

6. How can I be safer online?

- Always make purchases through well-known, trusted companies. Research the site before purchasing if you are unsure. Avoid sites that seem untrustworthy or have poor reviews.
- Use tokenized payment methods like Google Pay™ and Apple Pay™. These replace your card details with a unique token, reducing the risk of your payment credentials being leaked.
- Use the Digital Card with a dynamic CVV (Card Verification Value). This feature changes the CVV every 24hrs, making it harder for fraudsters to use your card details even if they manage to obtain them.

Where to get more help.

Additional Support Services.

- Scamwatch – create an account via ***scamwatch.gov.au*** and receive your credit report from ***equifax.com.au*** to ensure no false lines of credit have been applied for.
- Accessibility support – If you are deaf and/or find it hard hearing or speaking with people who use a phone, you can reach us through the National Relay Service (NRS). To use the NRS you can register at ***accesshub.gov.au/about-the-nrs***
- Lifeline – Lifeline provides all Australians experiencing a personal crisis with access to 24-hour support and suicide prevention services. Call Lifeline 24-hours on ***13 11 14.***

BankSA services.

Criminals constantly look for ways to steal your money and personal information. Remember, BankSA will never send you any links requesting your personal or financial information or ask you to share your password or Secure Code, install software to connect to your device or send you a link that directly opens our logon page.

Explore our Security Centre for regularly updated educational resources.

Visit ***banksa.com.au/security***

bankSA

Fraud Money Back Guarantee: Our BankSA Fraud Money Back Guarantee ensures that you will be reimbursed for any unauthorised transactions provided that you have not contributed to the loss and contacted BankSA promptly. Refer to your card's conditions of use for full details, including when a customer will be liable. This information is general in nature and has been prepared without taking your personal objectives, circumstances and needs and into account. You should consider the appropriateness of the information to your own circumstances and, if necessary, seek appropriate professional advice. Google Pay is a trademark of Google LLC. Apple Pay is a trademark of Apple Inc., registered in the U.S. and other countries.