BOS Banking Ombudsman Scheme

Quick Guide

Common scams targeting bank customers

15 June 2017

Scams targeting bank customers are becoming more sophisticated and more common. Despite that, following some basic precautions will keep your money safe from scammers. If you do become the victim of a scam and complain to us, our job is to determine whether your bank is liable for the loss.

Simple ways to bank safely

You always need to be on your guard when it comes to banking and money matters. That doesn't mean being suspicious or paranoid. Rather, it means exercising care and maintaining a healthy scepticism towards individuals or companies when you're online. We recommend you take the following precautions:

- Find out something about the company or individual you are dealing with. Do an internet search, look for reviews, ask for a physical address you can check, and look up the company on the Companies Register.
- Check Consumer Protection's scam alert website.
- Check with someone independent and trustworthy before you commit to anything.
- Do not give out account details unless the business is established and trusted.
- Never accept money into your account for subsequent transfer to others.
- Never give out your PIN or internet banking password.
- Check your accounts regularly to ensure money is going to the right places.
- Report any likely scams to your bank.
- When emailing people about making a payment, confirm the payment details using another form of communication (such as by phone). You may not be communicating with the person you imagine, because fraudsters hack into email accounts and assume the account holder's identity. A quick phone call can foil such deception.
- Contact your bank immediately if you suspect you have been scammed. It may be able to reverse a payment (but that's unlikely if you've authorised the payment and it has gone through).

Phishing Scams

Scammers try to trick customers into giving out personal information such as bank account numbers, passwords and credit card numbers. This is called a phishing scam. Typically, customers receive an email from what looks like their bank. It will say they need to confirm some personal details, usually their internet banking username and password. It will contain a link to a website that looks like the bank's but is fake. Customers who enter these details will soon find scammers have accessed their accounts and cleared out their money.

Be *extremely* wary of emails that appear to be from your bank and that ask you to confirm your personal details. Banks will *never* ask you for your password in emails. Don't click on links within any email if you have the slightest suspicion about its authenticity. Simply delete the email. If you need to go to your bank's website, type the address into your browser.

If you enter your internet banking password and other details into a fake website, it's likely you will be liable for any losses because you disclosed this crucial information.

Fraudsters may also make phishing phone calls pretending to be your bank, telephone company, government department, or a computer company. They may ask you to turn on your computer and download software that gives them access to everything on your computer. A fraudster who has gained access to your computer may be able to steal money from your bank accounts. Be very cautious about unsolicited phone calls, no matter how plausible the caller sounds.

Sending money to scammers

Scammers can also trick bank customers into sending money to them. How they do this varies. A common way is to ask customers to send a processing fee in order to receive an inheritance or the proceeds of an investment. Another is for someone met on an online dating site to seek financial help. Losses from such scams can run into tens of thousands of dollars.

Always be careful if someone you don't know or have met only online asks for money. It can seldom be recovered. Your bank is very unlikely to be liable for losses you suffer if you give it instructions to send money to someone, it follows those instructions and you later find out that the individual was a scammer.

Money mules: sending someone else's money to a scammer

Another scam is to ask a bank customer – the mule - to accept and forward on money stolen from another victim's bank account. Scammers convince people there is a legitimate reason for the transfer, such as paying a fee associated with a job application or helping someone with whom they have an online relationship.

A bank may reverse a payment into a mule's account if the money is found to have been stolen. This, in turn, can cause the mule's account to be overdrawn if there isn't enough money in the account. The bank will ask the mule to repay the overdrawn sum.

In such cases, we consider whether the bank's terms and conditions allow it to reverse a payment from a mule's account. We also assess whether the bank had sufficient information to conclude the money was stolen before it reversed the payment. If so, the customer will be held liable for the loss.

PIN scams

These aim to get customers to disclose their PIN. Scammers have usually already stolen a customer's wallet, but to use any credit or debit cards they need the PIN.

Scammers use different techniques to get intended victims to disclose their PIN. Scammers may, for example, say they are from the bank and have noticed suspicious transactions that indicate a card has been stolen. They will suggest cancelling the card, but doing that, they add, will require the customer to verify his or her PIN in order to authorise the cancellation. The giveaway here is that banks *never* ask for customers' PIN.

Another technique is to contact a customer and say he or she has won a prize. The customer is asked to make up a four-digit number for identification purposes when collecting the prize. The scammer may be making the call from an ATM and will tap in the number. If not the PIN, the scanner will say that number has been taken, and to pick another. Subconsciously or otherwise, many customers will eventually give over their PIN.

By disclosing your PIN to anyone, you are breaching the terms and conditions of your account or card and you will generally be liable for fraudulent transactions. You won't be liable for fraudulent transactions if you have taken reasonable care of your card and PIN.

See also our quick guides on:

- Looking after your credit and debit cards and PINs
- ATMs
- Contactless technology

Case 1: Victim takes bait in series of nibbles

Mr F began corresponding with Ms B through an online dating site. After several months, Ms B told him she was moving to Ghana. Later, she emailed saying she needed him to buy her a laptop to replace one stolen when she arrived in Ghana. He did so, and sent it to the address she had supplied.

Ms B then began requesting money for other things. She managed to convince him to call the bank and instruct it to transfer money to an account in Britain in the name of a Mr W. On four separate occasions, Mr F transferred money to Mr W's account.

When Mr F realised he had been defrauded, he contacted his bank. He believed it should have alerted him to the possibility the recipient was a fraudster and should have prevented the transfer of $43,972 to the account. In Mr F's view, banks should query customers about transactions involving the transfer of large sums overseas.

The bank said it could not have known the transfers were suspicious, and was not responsible for losses from transactions he authorised.

We had to determine whether the bank was liable. We were satisfied it was unaware Mr F might have been the victim of a scam: it could not therefore have warned him about something it did not know about.

The bank was also unaware Mr F had met Ms B on an internet dating site. He gave bank staff the impression Ms B was a trusted friend. He gave a plausible explanation about the intended use of the money. When a bank employee queried the transfer to Ms B via Mr W's account, an unusual practice, he appeared unconcerned. Mr F also said he appreciated that Ghana was not the best place to which to be sending money.

In reviewing information, including phone calls between Mr F and bank staff, it was clear Mr F requested and authorised the payments to the British account. We considered that, even if warned about the possibility of fraud, he would possibly still have made the payments because he strongly believed Ms B was genuine.

The fraudster, by starting with the transfer of a relatively small amount, had set out to establish a track record between Mr F and Mr W, enabling subsequent larger transactions to take place without raising bank staff suspicions.

Case 2: Transfer "job" leaves debt of more than $3,000

Mr A had been unemployed for two years when he received an email from a stranger offering employment as a mystery shopper. He replied with the requested contact details and the name of his bank, and received his first assignment – transferring money to an account in Nigeria.

Despite having suspicions, Mr A decided his bank would intervene if it had any concerns about the transactions and so followed instructions. He gave out his bank account number, and $3,000 was soon paid into his account. He immediately transferred $2,700 to the Nigerian account, leaving him with a payment of $300.

But soon after he transferred the money, his bank discovered the $3,000 deposit had been fraudulent and reversed it. Mr A was left with a $2,700 debt and blamed the bank, believing its security systems should have protected him from unauthorised access of his account.

Allowing the deposit of $3,000 into his account after freely disclosing his account details is not unauthorised access and is outside the bank's control. The unauthorised access was into the account of a customer from another bank from where the fraudsters stole the $3,000 they transferred via him to another individual.

Mr A believed the transaction was legitimate, but we did not consider this was a reasonable view, given the circumstances of the "job offer" and his initial suspicions. The bank's terms and conditions allowed for transaction reversals in cases of money laundering. We therefore concluded the bank was entitled to reverse the transaction.

Mr A's $3,000 debt was, meanwhile, increasing further in the hands of a debt collection agency. With our encouragement, the bank agreed to recall the debt and accept a lump sum payment of $3,200 – about $1,000 less than Mr A would have had to pay the collection agency.

Case 3: Carelessness with PIN costs dearly

Mrs M took a call at work from someone saying she had won a $1,000 AA gift voucher. The caller asked for a four-digit password to redeem her voucher. She said she suggested three, and each time the caller said they were already taken. She said the caller then gave her a random number to use. In reality, the call about a winning voucher was simply a trick to try to get the PINs for her cards. How the caller obtained her PINs was later a matter of dispute.

Unknown to her, her handbag containing two debit cards had been stolen from work. The offender made purchases and withdrawals exceeding $6,000. When Mrs M realised her handbag was gone, she cancelled her cards and asked the bank to reimburse the offender's spending.

The bank said it was not liable because she had not taken care of her cards as specified in her accounts' terms and conditions. She had left her bag in an unsecured place and had been careless

with her PINs (which were the same for both cards). It said she must have disclosed her PIN to the offender when she proposed the voucher passwords. She disputed that, saying the caller had somehow deciphered her PIN from her suggested password numbers. Our investigation, however, suggested otherwise because:

- She had told the bank she might have given the offender her PIN.
- She told Police she had done so.
- The offender entered her PIN correctly on the first attempt for both cards, which usually indicates fraudsters have obtained the PIN from cardholders.

We thought it likely Mrs M had used the same password not just for both cards (each of which should have a unique number for better security) but also for a variety of non-banking-related purposes. This, too, was an unsafe practice. Given this, we encouraged Mrs M to reconsider the bank's offer – of reimbursing half of her loss as a goodwill gesture – because it seemed very likely she had contributed to the theft by revealing her PIN. Mrs M accepted our view and took the bank's offer.