# Helping you to protect yourself against fraud and financial crime

**HSBC takes fraud and other financial crimes very seriously. Even though we have market-leading fraud detection systems, we want you to be aware of the different ways criminals may try to steal not just your money but also your identity.**

Here are a few tips on how to avoid becoming a victim of fraud and other financial crime. Please read in conjunction with our Banking Made Easy and HSBC Terms and Conditions.

**"Vishing"**
This involves a fraudster making phone calls to a victim, posing as bank staff, the Police and other officials or companies in a position of trust. The call may be made to coerce the victim into:

- Sending their money to another account often purportedly for 'safe keeping' or 'holding';
- Withdrawing cash and handing it over to the fraudster for investigation;
- Giving personal financial information, which can then be used to gain access to their victim`s finances.

Remember,

1. Be wary of unsolicited approaches by phone, especially if asked to provide any of your personal information.
2. If you are suspicious or feel vulnerable, don't be afraid to terminate the call and, say no to requests for information.
3. It takes two people to terminate a call, so ensure the caller has also hung up and you have a clear line, you can use a different phone line to test the number.
4. Fraudsters can use 'call spoofing' to deliberately falsify the telephone number relayed on the caller ID to show as a genuine bank number.
5. HSBC will never call you to ask you to generate a Secure Key code by pressing the yellow button or ask for your PIN number.
6. Never share your security details with a third party. It is important to keep your account and security details safe.

Criminals may already have basic information about you in their possession (ie, name, address, account details), do not assume a caller is genuine because they have these details or because they claim to represent a legitimate organisation.

**Courier Scams**
Rather than telling you to destroy your card, some fraudsters arrange for a courier to come round to your house to collect the card. They may also ask you to write down your PIN and hand it to the courier. To add credibility the fraudster may even advise you to cut the card in half. Please note that:

- We will NEVER ask for your card and PIN to be returned via courier.
- You should NEVER divulge your PIN to anyone, even someone claiming to work for the bank.
- HSBC's fraud detection teams will only ask for partial information, so for example, they will never ask for full mother's maiden name or full date of birth.
- To ensure that we can make prompt contact should anything look untoward on your account, please provide HSBC with up to date contact details including a mobile telephone number.

**"Phishing"**
This is where people receive e-mails directing them to websites where they are asked to provide confidential personal or financial information. Whilst these e-mails may appear to come from a legitimate site, these emails are designed to steal your personal information and use it to access your accounts. This is known as Phishing. Do not reply or click on a link in an e-mail that warns you that your account may be shut down unless you confirm your personal information. Instead contact the company, in a way that you are sure is genuine such as an authenticated telephone number.

You should delete these e-mails immediately.

**Letting others use your account**
Criminals may also try to take advantage of the fact that HSBC sometimes allows you to withdraw funds before any cheques paid in have cleared. This scam can be targeted at younger customers who are tricked into paying in a cheque by someone else they consider to be a "friend". Pressure can then be applied for the funds to be withdrawn before the cheque has fully cleared and an overdraft could be created when the cheque is returned unpaid.

Fraudsters may also advertise for people to receive funds (and sometimes goods) on behalf of charities abroad. The idea is that you pay funds into your account, which you pass on after deducting your commission. Unfortunately these funds may be the proceeds of their crimes. The handling or concealing of criminal money may result in a person being found guilty of an offence in a court of law.

DO NOT allow anyone else to use your card, PIN, password or other security information.

**Investments/Boiler room Scams**
This type of scam involves a fraudster making a cold-call to potential investors offering them worthless, overpriced or even non-existent shares. These can come in many forms however there are a number of common factors you should look out for including:

- Unsolicited approaches.
- Unrealistically high returns offered for "low risk" investments
- Lack of independent evidence of the validity of the scheme.
- Pressure to make quick decisions.
- Instructions to keep the approach confidential.
- Telephone numbers quoted are often untraceable mobiles.

Remember: If it sounds too good to be true - it usually is!

**Pension Liberation**
This involves the transfer of a pension from an existing scheme to a new one, with the intention of allowing early access to benefits before the legal age of 55. These individuals might be under financial pressure and the fraudster will sometimes advise that they can unlock some or all of their pension fund for a fee, which can be very high and may result in serious tax consequences. Be alert to offers like this and if in doubt seek advice from registered pension providers.

**Protecting your Card**
- Sign and activate your new card as soon as you receive it.
- You can activate your card either through internet banking, by calling us (using the number in the useful contacts below) or by using an HSBC ATM (for Visa debit cards, unless a new PIN has been issued).
- Contact us (using the number in the useful contacts below) if your replacement card does not arrive a week before your old one expires.

**Protecting your PIN**
- Never write down or otherwise record your PINs and other security details in a way that can be understood by someone else.
- Destroy your PIN advice as soon as possible.
- Choose a PIN number that cannot be associated with you and isn't a sequence such as 1234 or 1111. Ideally choose a random combination or a sequence of numbers which are important to you.

**Protecting yourself at the ATM**
- A device may have been fitted to the ATM, which could enable the fraudster to steal your card or capture the information contained within the magnetic strip. If you notice anything unusual attached to the ATM, do not try to remove it. Move away from the machine and call our Lost and Stolen Cards team (using the number in the useful contacts below) or the police.
- Always stand close to the machine and use your hand as a shield over the keyboard. Criminals may try to watch you entering your PIN, before trying to steal your card.
- If the cash machine does not return your card, do not re-enter the PIN. Report the loss of your card to our 24 hour Lost and Stolen Cards team (using the number in the useful contacts below).

**Protecting yourself over the Telephone**
- When making card payments over the phone, you should have your card in front of you as you may be asked information such as expiry date, issue number and the three-digit security code on the signature strip. However, NEVER divulge your PIN over the telephone, even if asked.
- Try to avoid saying your card information in public places where people may overhear.
- Request postal or email confirmation of the transaction.

**Protecting yourself whilst Shopping**

- Try to use your hand as a shield when entering your PIN.
- If you encounter any problems whilst using your card, please call our Customer Telephone Service team (using the number in the useful contacts below).
- Please keep your cards in a secure place at all times.

**Protecting yourself Online**

- Only shop at secure websites – ensure that the security icon (a locked padlock) is showing in the browser window if on a page requesting input of personal information. Get Safe Online (address below) provides further guidance and support on this topic.
- Print a copy of your order confirmation. A postal address and telephone number should also be available.
- When paying online with a credit card, always sign up with Mastercard Securecode or Verified by Visa. These provide personal password protected services.
- Download HSBC Rapport software, from our online banking security page; please find full details of this product via our Security Centre (using the website address in the useful contacts below). Please read the Rapport Software Terms and Conditions prior to installing.

**Protecting your Passwords**

- Use different passwords for different systems.
- Do not be tempted to use passwords that can easily be guessed such as children's names or birth dates.
- Never write down your passwords, however if you have no alternative, record them in a way that cannot be understood by anybody else.
- Instead of using your Mother's Maiden as your memorable name, consider using the name of your favourite cartoon character or another fictional person.
- Use a mixture of numbers and letters of upper and lower case to strengthen your password.

**…And protecting yourself against Identity Theft**

Using a variety of methods, criminals may obtain important pieces of personal and identity data such as credit card numbers, expiry dates, dates of birth or mothers' maiden names. This information can be used to gain access to bank accounts or open new credit facilities.

Help to avoid this by following these simple steps:

- Shred all receipts or any letters, which contain your name and address or other personal information. Switch off your postal statements to prevent unnecessary documents being sent via the mail.
- Set up a telephone security number, as this is a secure way for us to identify you when you call us.
- Don't give your telephone security number out to anyone who contacts you. HBSC will NEVER ask for your telephone security number if WE call YOU.
- If you have lost or had stolen important documents such as a passport, consider registering for the CIFAS Protective Registration Service (see link below).

**Useful numbers and addresses**

**Customer Telephone Services**
(Please call this number in the first instance)
**03457 404 404** or if overseas **44 1226 261 010**
Textphone **03457 125 563** or if overseas **44 1792 494 394**

**Security Reset Team** (Please call this number if suspect you may have divulged your security details) **0345 600 2290**

**Lost or Stolen Cards**
**03456 007 010** or if overseas **44 1442 422 929**

**www.hsbc.co.uk/security**
**www.cardwatch.org.uk**
**www.chipandpin.co.uk**
**www.fca.org.uk**
**www.cifas.org.uk**
**www.equifax.co.uk**
**https://secure6.arcot.com/vpas/hsbcdebit**
**https://enrollment.securecode.com/vpas/hsbcus.html**
**www.identitytheft.org.uk**
**www.getsafeonline.org**
**www.actionfraud.police.uk**
**www.financialfraudaction.org.uk**
**www.cyberstreetwise.com**

**hsbc.co.uk**

**Issued by HSBC UK Bank plc**
Customer information: PO Box 6201, Coventry CV3 9HW