first direct

Helping you to protect yourself against fraud and financial crime

first direct takes fraud & 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.

If you suspect that you may have been tricked into divulging your security details or you notice anything suspicious regarding your account, please call us as soon as possible on **03 456 100 100** (Text-phone **03 456 100 147**) or if you are calling from abroad, **+44 113 234 5678** (text relay **+44 151 494 1260**).

Here are a few tips on how to avoid becoming a victim of fraud and financial crime.

Protecting your Card

- sign your new card as soon as you receive it;
- safely destroy any Card PIN advice we send you immediately after receipt e.g. by shredding it;
- keep your debit card separate from your cheques;
- contact us if your replacement card does not arrive a week before your old one expires;
- do not tamper with the card;
- do not disclose the card number, Card PIN or card security codes except when using the cards to make payments.

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 you Card 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;
- do not disclose your Card PIN for mail order payments or when paying for goods and services over the telephone or through the internet.

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 us 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 Call Centre.

Protecting yourself over the Telephone

- 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;
- ask the retailer to confirm the full price being charged, including booking fees or delivery charges;
- raise any discrepancies directly with the retailer; however you should contact us if you cannot resolve any issues;
- try to avoid saying your card information in public places where people may overhear;
- request postal or email confirmation of the transaction;
- when contacting us by telephone, you should not use a cordless or mobile telephone operating on an analogue network. We recommend that you use either a landline telephone or a digital mobile telephone.

Protecting yourself whilst Shopping

- try to use your hand as a shield when doing so. The PIN, along with a microchip set into your card, will make using your card far more secure;
- occasionally, the retailer may be required to ask you some security questions to make sure your card is not being used without your permission. NEVER divulge your PIN;
- if you encounter any problems whilst using your card, please call us;
- never leave your cards lying around.

Protecting yourself Online

- only shop at secure websites – ensure that the security icon (a locked padlock or broken key symbol) is showing in the browser window. Print a copy of your order confirmation. A postal address and telephone number (not a mobile) 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;
- keep your personal computer secure by using anti-virus and anti-spyware software and a personal firewall;
- download Rapport software, more information about this can be found on our Trusteer Rapport page. Please ensure that you read Trusteer's Terms and Conditions prior to installing Trusteer Rapport software, as we are not responsible for any errors or omissions of their product;
- always access Internet Banking by typing in the bank address to your web browser, never go to Internet Banking from a link in an email and then enter personal details;
- never access Internet Banking from any computer connected to a local area network (LAN) (this is usually the case for computers you use at work) or any public internet access device or access point (e.g., at an internet cafe) without first making sure that no one else will be able to observe or copy your access to get access to Internet Banking pretending to be you;
- once you have logged on to Internet Banking, do not leave the electronic media from which you have accessed it or let anyone else use the electronic media until you have logged off.

Protecting your Passwords

- keep your security details unique to your accounts with **first direct**;
- do not be tempted to use passwords that can easily be guessed such as children's names or birth dates;
- take care to ensure that no one hears or sees your security details when you use them;
- never write down your passwords, however if you have no alternative, record them in a way that cannot be understood by anybody else.

...And protecting yourself against Identity Theft

Using a variety of methods, including raiding dustbins for credit card slips and bank statements or obtaining data from public records, criminals can 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 "impersonate" victims and 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. Go paperless to reduce the number of paper statements with your personal details on;
- don't give your password out to anyone who contacts you – even if they claim to be from your bank or the police. We will NEVER ask for your password if WE call YOU;
- do not allow anyone else to have or use your card, PIN or any of your security devices, details or password(s) (including for Internet Banking and Telephone Banking) and do not disclose them to any third parties, including the police or account aggregation services not operated by us. You can disclose your card number and other card details when using your card in connection with making payments;
- never record any password details on any software which retains it automatically (e.g. any computer screen prompts or 'save password' feature or the line on your internet browser) unless retaining your password is a specific function of a banking service provided by **first direct** such as the Internet Banking Plus service;
- if you have lost or had stolen important documents such as a passport, consider registering for the CIFAS Protective Registration Service through Equifax on **0870 010 2091**. This will help prevent fraudsters using this documentation to impersonate you.

Courier Scams

Rather than telling you to destroy your card, some fraudsters are arranging for a courier to come round to your house and 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;
- our Fraud Detection Teams will only ask two of your security questions if they contact you;
- to ensure that we can make prompt contact should anything look untoward on your account, please provide **first direct** with your up to date contact details including a mobile telephone number.

"Phishing"

Increasingly, people in the UK are receiving e-mails that direct 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, they only have one purpose and that is 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. 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.

“Vishing”

This involves a fraudster making phone calls to a victim, posing as bank staff, the Police, official persons or companies in a position of trust. The call is made either to coerce the victim into sending their money to another account often for ‘safe keeping’ or ‘holding’, to withdraw cash and hand over for investigation, or to obtain personal financial information, such as Internet Banking logon details or answers to security questions which are then 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, 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, use a different phone line to test the number.
4. Fraudsters often use ‘call spoofing’ to deliberately falsify the telephone number relayed on the caller ID to show as a genuine bank number.
5. **first direct** will never call you to request codes from your Secure Key, ask you to generate a code by pressing the yellow button or ask for your PIN number.
6. Never share your security details with anyone. It is important to keep your account and security details safe.

Criminals may already have basic information about you in their possession (i.e., 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.

Letting others use your account

Criminals may also try to take advantage of the fact that **first direct** sometimes allows you to withdraw funds before any cheques paid in have cleared. This scam is often targeted at younger customers who are tricked into paying in a cheque by someone else they consider to be a “friend”. Pressure is then applied for the funds to be withdrawn and as the bank may allow access to the funds 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 a person being found guilty of money laundering. 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 cold-calls to potential investors offering them worthless, overpriced or even non-existent shares.

Boiler room scams use sophisticated tactics to approach investors offering to buy or sell shares in a way that they say will give investors a huge return. Share fraud usually comes out of the blue, with scammers cold-calling investors after taking their phone number from publicly available shareholder lists. But the high-pressure sales tactics can also come by email, post, word of mouth or at a seminar.

These scams are sometimes advertised in newspapers, magazines or online as genuine investment opportunities. They may even offer a free research report into a company in which you hold shares, a free gift or a discount on their dealing charges. You will often be told that you need to make a quick decision or miss out on the deal. The scammers might also try to sell you shares in a company you have never heard of, often because it does not exist. If you buy these shares, it is likely you will be left with a worthless investment.

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 are often under financial pressure and will be advised that they can unlock some or their entire pension fund for a fee, which can result in serious tax consequences.

Useful numbers and addresses

Call Centre
03 456 100 100 (Text-phone: **03 456 100 147**)
or if calling from abroad **+44 113 2345678** (text relay: **+44 151 494 1260**)

Police (999)

CIFAS Protective Registration Service through Equifax
0870 010 2091

www.firstdirect.com/1/2/security-centre
www.firstdirect.com/1/2/security-centre/trusteer-rapport
www.cardwatch.org.uk
www.chipandpin.co.uk
www.fca.org.uk
www.cifas.org.uk

If any card, PIN, security device or security details are lost or stolen, or you suspect that someone has used or tried to use them, you must tell us without delay.

If asked, you must confirm in writing the loss or theft of your cards or security details relating to your card, Internet Banking or Telephone Banking by writing to us at:

first direct
40 Wakefield Road
Leeds
LS98 1FD

We will ask you to co-operate with us and the police in relation to any investigation into the actual or suspected misuse of your card, password, PIN, security details and/or accounts. You must report any unauthorised transactions to the police within seven days of our request. We may also disclose information about you or your account to the police or other third parties if we think it will help prevent or recover losses.

CK-FDFG 06/18 (v2)