Fraud Awareness
Advice for Private Banking Customers

bba

The voice of banking
& financial services

Fraud Awareness

Helping you to protect yourself against fraud

There is now compelling evidence to show that fraudsters are targeting high net worth customers. When it comes to fraud, prevention is always better than cure. Increasingly more sophisticated methods are being used to commit fraud and it is important that you remain vigilant at all times to reduce the risk of becoming a victim of fraud. The banking industry is committed to supporting you fight the risk of fraud, protect your identity and safeguard your money.

Checks in place when contacting your bank

When you contact your bank or are contacted by your bank, depending on the nature of your request, you may be required to go through additional identity verification checks designed to protect you and your assets from fraud. For example, when providing new contact details or making a payment request you could receive a security call back to verify details, including security questions.

You should be certain that you are talking to a member of staff from your bank before you disclose your security identification answers or passwords. If you are in any doubt call your bank back on a known/advertised telephone number.

If you provide your bank with a payment instruction you may be asked for only two characters of your password rather than the full password.

Remember:

- Never write down or give your security identification answers of passwords to anyone unless you are certain you know who you are dealing with.
- Always ensure that banking, financial and valuable personal documents, such as passports, are stored securely.
- Always shred financial documents before you throw them away.

Types of fraud

Online and email fraud

As we become more dependent on mobile technology to keep up with our busy lives, the risk of having personal information compromised or accessed when using unsecured WIFI increases if you do not take the proper precautions.

Taking simple measures to protect yourself can help prevent others from capturing your passwords, accessing your private emails or downloading viruses onto your devices. The steps set out below will help you prevent this happening:

- Unless using a secured web page do not send or receive private information when using public WIFI, especially avoid financial transactions.
- Avoid accessing private information on public devices and always delete your browsing history.
- Install anti-virus software, anti-spyware and a firewall on your computer and mobile devices and keep the software up to date.
- Only make online purchases using secure websites – those with an address beginning with https:// where the padlock symbol is displayed.
- Research any online retailer you are unfamiliar with to ensure they are reputable.
- Do not reply to unsolicited emails from companies you do not recognise.
- Do not click on links or download attachments that you are not expecting to receive.
- Keep your receipts.
- Check credit card and bank statements carefully after shopping to ensure that the correct amount has been debited, and also that no unauthorised transactions have been processed.
- Challenge anything you don't recognise immediately.

Investment fraud

Investment frauds generally target individuals with a chance to invest in a company or opportunity which appears to offer very high rates of return:

- These criminal organisations will have well trained, highly professional sales people who can be very persistent, and often use high pressure "closing techniques" such as "this is your last chance, tomorrow will be too late." They try to isolate you from taking advice by saying "I'm going to have to insist you sign a non-disclosure or confidentiality agreement before we can discuss this further."
- Be wary of organisations that cold call, write or email you about investments opportunities. Do not let a glossy brochure or website trick you into thinking that the approach is from a legitimate or credible company.
- Do not be afraid of hanging up on cold callers asking you to invest and do not respond to unsolicited emails or letters asking you to invest or send a fee to facilitate a prize release or investment opportunity.
- Contact your Client Advisor to discuss such "opportunities" if you receive a proposition.
- If you believe you have been a victim of investment fraud or you believe your details may have been added to a register of "targets/victims" you can contact your Client Advisor for guidance and/or contact the Financial Conduct Authority Consumer Helpline or the Police via the Action Fraud website.

ATM Fraud

You should remain vigilant to the risk of bank cards and PIN codes being stolen or compromised when using an ATM:

- Do not get distracted when using your card at a cash machine and always cover your hand when entering your PIN code to prevent anyone seeing the number.
- If you notice anything unusual about the cash machine, use an alternative machine.
- Do not allow retailers to take your card out of your sight.
- Use a separate PIN code for each card, in “difficult to guess” combinations.
- Never tell anyone your PIN code, even if they claim to be from the relevant bank or from the Police. If a caller asks you to key your PIN code into the telephone key pad always refuse.
- Never allow an apparent bank official, law enforcement officer or courier to collect your card on the premise that your card needs to be replaced.
- Contact your card provider immediately if your card gets retained by an ATM or if you think your card has been compromised, lost or stolen.

Be vigilant and take action if:

- You receive bills, invoices or receipts for goods or services you have not ordered.
- You haven’t received your usual bank/credit card statements.
- There are times on your bank or credit card statements that you don’t recognise.
- Important documents, such as passports or driving licenses, have been lost or stolen.
- You received an unexpected or unexplained telephone call claiming to be from your bank or another financial institution.
- You receive unexplained letters regarding outstanding debts from solicitors or debt collectors and/or financial institutions that you do not have a relationship with.
- You have a good credit history, but are refused a financial service or product.
- You get an approach which is “out of the ordinary”, such as a prize win. Never respond, provide personal information or send any payment.

If you think you are a fraud victim:

- Contact your Client Advisor.
- Check that your address, telephone numbers and email address records with us are correct.
- Change your security identification answers and passwords, if you believe these may be known by others.
- Check your account statement carefully to gauge the extent of the problem.
- Notify any other financial institutions that you have relationships with.
- Consider checking your credit status with a credit agency such as Experian or Equifax.
- Consider obtaining a protective registration marker from CIFAS, the fraud prevention agency.

Useful external contacts:

www.actionfraud.police.uk

www.cifas.org.uk

www.equifax.co.uk

FCA Consumer helpline: 0800 111 6768
www.fca.org.uk/consumers/scams

www.getsafeonline.org

For More Information on
Fraud awareness please contact:
Matthew Allen
Director Financial Crime
on matthew.allen@bba.org.uk