Hampden & Co.
BANKERS

Banking Safely

Section 1
How Hampden & Co helps protect you from fraud

Keeping your finances and personal information safe is crucially important to Hampden & Co. In this document we outline how to keep you and your finances safe and if you would like to find out more, or if you have any concerns about these matters, please speak to your Private Banker straight away.

Firstly, you should know that no one at Hampden & Co will ever ask you:

- Your PIN.
- Your Digital Banking password.
- Your One Time Password which is generated for logging onto Digital Banking and for creating payments.
- The 3 digits on the back of your debit card or charge card (CVV number).

When you call our Cards Centre, if you have lost your debit card for example, you will be asked for answers to the security questions which were set up for this purpose when you opened your account.

We will never ask you to move money to a so-called "safe" bank account or to a new bank account.

We do not send you confidential information by email unless it is encrypted.

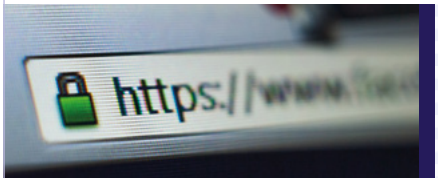
If you are worried that you may have been a victim of fraud or have any concerns that your personal information, account details or mobile device may have been stolen, it is important that you contact our Cards Centre or your Private Banker right away. We recommend as best practice that you add your Private Banker's contact details and the Card Centre number to the contacts on your mobile phone to allow you quick access to these when required.

www.hampdenandco.com/contact-us

Section 2
Steps to help you protect yourself

There is a great deal of coverage in the media about the different ways that criminals use to try to steal money or information. There are a few straightforward steps that everyone can take to minimise their risks from these attempts, which we have detailed below.

- Keep your security details, passwords, PIN details and any Internet Banking details secure and do not share them with anyone else.
- When making a card transaction keep your card in your possession and do not let the card out of your sight. It is very unusual now to be asked to take your card away, and if this does happen simply ask to join the person at the card machine.
- Let your Private Banker know if you change address, email or phone number so that the information we have is accurate.
- Check your bank statements regularly and let us know of any transaction that you do not recognise.
- Shred anything containing personal data when you want to throw it away.
- At cash machines and when making payments, take care when others are close by as they may be trying to see you enter your PIN. If you think someone may have seen your PIN, you can change it at most cash machines.
- Be aware that your post is valuable information in the wrong hands. If you don't receive a bank statement, card statement or any other expected financial information, contact us, or the relevant organisation.
- Do not respond to emails requesting information (account numbers, card details, PIN or passwords). We will never request information from you by email and it is our policy not to send personal data to you by email – there is more information on this type of scam, called "Phishing" below.



Section 2
Steps to help you protect yourself (cont)

- Remember that email communication is not secure so please do not send us confidential information this way. Secure messaging is available within our Digital Banking system, or just give us a call.
- We will never ask you to move money to a so-called safe bank account or to a new bank account.
- We will never ask you to download remote access software (such as TeamViewer) on to your computer or mobile device.

a) Take care when making payments

Be careful when you make a payment online or give your Private Banker a payment instruction. Pay attention to warnings and security measures (e.g. one-time passwords) when:

- Setting up a new payee.
- Amending an existing payee.
- Immediately before authorising a payment.

Before authorising your payment:

- Check the payee is who you are expecting to pay.
- Check the amount.
- Ask yourself how confident you are that you are paying for genuine goods/services/investments.
- Ask yourself if you have done enough to confirm that the person or business you are paying is legitimate.
- Do not rely on the payment details you have been sent, for example in an email, as these could have been intercepted and changed. Call back the payee on a number you know.
- If you are a micro-enterprise or charity you must follow your own internal procedures for the approval of payments.

Please remember that fraudsters are very good at tricking people. If we contact you by phone to confirm payment details of a new payee, please make sure you are entirely confident that the payment information is true and correct, otherwise we may not refund your money if it turns out to be a scam. There is more information on this type of fraud called an "authorised push payment scam" in Section 3 below, and how you can avoid them. If you have any doubts, don't make the payment.

Fraud refunds

- The steps above help prevent you from authorising payments to fraudsters and give you the chance of a refund if the payment turns out to be a scam.
- We look at all cases of fraud on a case by case basis to make sure you took care when making the payment. We can then decide whether to refund you for any money you may have lost.
- We may not give a refund if you do something dishonest, obstructive or careless that helps an instance of fraud take place.

b) Keep your bank cards, cheque books and security details safe

- Do not share your security details, passwords, PIN details and any Digital Banking details with anyone else (even a joint account holder).
- Use passwords that are not easy for other people to guess.
- If your card is retained by a cash machine or any other payment machine, please notify your Private Banker or the Card Centre immediately to block the card.

c) Keep safe online

Install and keep up-to-date antivirus software on your computer and keep your operating systems up to date when rolled out by providers.

d) Do not act as a money mule

Do not act as an intermediary for the receipt and payment of funds – you might become a "money mule" for criminals and be guilty of money laundering.

Further information on what is a money mule and how to protect yourself from becoming a mule can be found on:

www.moneymules.co.uk

Section 3
Examples of common frauds

There are several common methods that criminals use. We have put some examples below to help you identify when you may be at risk from a fraud and the action you should consider taking. If you have any concerns that you might have been a victim of fraud, please let your Private Banker know straight away so that they can help you or contact our Cards Centre if card related.

www.hampdenandco.com/contact-us

If you have been a victim of fraud or cyber-crime, you should think about reporting it to Action Fraud.

www.actionfraud.police.uk

Payment fraud – Authorised Push Payments (APPs)

Scams involving APPs occur when someone is tricked into authorising an electronic payment from their bank account to an account that they believe belongs to a legitimate payee but is in fact controlled by a scammer.

Payments related to APP scams can be made over the phone, online, or in person, and most are completed instantly.

Examples of APP frauds

- Property transactions – criminals intercept the email chain between sellers, buyers, estate agents and solicitors. The fraudsters change the payment information related to transfer of funds so that payments are diverted to the fraudster's account.
- Fraudsters who convince people to move money to a "safe" account such as another bank account.
- Invoice scams – where fraudsters send a false invoice, often pretending to be from a company from whom you are expecting a bill.
- Romance scams – fraudsters form a relationship in order to ask for money, or enough personal information to steal your identity.
- Purchase scams – sending money to buy goods or services that do not exist.

  This is one of the most prevalent frauds according to UK Finance. See their website for further information.

Payment fraud – debit and charge cards

This is where fraudsters use stolen debit, credit or charge cards, or their details, to buy goods or services.

If your card is taken by a cash machine, or another payment machine such as parking machines/meters, please call our Card Centre immediately so they can block your card. Your card may have been retained by the machine legitimately due to a fault but occasionally fraudsters will attach card trapping devices to cash machines and as soon as you leave the machine the fraudster will remove the card from the slot and use the card for fraudulent transactions. Our Card Centre will cancel your card straight away and arrange for a new card to be ordered.

We provide an extra layer of security when you are shopping online with your Hampden & Co debit or charge card. You may be asked to enter a One-Time Password (OTP) in order to confirm that your purchase is genuine. We will send a unique OTP by text message which will then be entered by you into the website you are using for the purchase. If you receive an OTP that you are not expecting please advise us immediately.

Phishing

Phishing is the fraudulent practice of sending emails or phoning and claiming to represent reputable organisations (e.g. a bank, social media site, TV Licensing, HMRC etc) and requesting personal information such as your bank details for verification or recording purposes.

Malware

Malware is short for "malicious software" which has been specifically designed to disrupt, damage or gain unauthorised access to a computer system. Any electronic device, including phones and tablets, can receive malware. Your device can become infected if you click on links or download software or files from suspicious websites and emails.

Identity fraud

Identity theft occurs when a fraudster steals your personal information or possessions so they can use your identity for their own financial gain. Phishing and malware are often the means of capturing this data.

Once a fraudster has enough information, they can use your identity to:

- Open bank accounts.
- Take over existing bank accounts.
- Obtain genuine documents.
- Borrow money.

Section 4
Useful links

There is much more information available about how you can keep your data and your finances safe, and we have selected links to some of the best of these.

- **"Take Five" to stop fraud**
  takefive-stopfraud.org.uk

  Take Five is a national campaign that offers straight-forward and impartial advice to help everyone protect themselves from preventable financial fraud. It is led by Financial Fraud Action UK (part of UK Finance) and backed by the UK Government. Further advice and information can be found in the Take Five Customer Advice Guide.

- **The Financial Conduct Authority**
  www.fca.org.uk/scamsmart

  Find out how to protect yourself from investment scams and how to check you are dealing with an authorised firm.

- **The Financial Services Register**
  register.fca.org.uk

  This is a public record of all firms, individuals and other bodies that are regulated by the Financial Conduct Authority.

- **Get Safe Online**
  www.getsafeonline.org

  Get Safe Online is a source of unbiased, factual and easy-to-understand information on online safety. This contains lots of information on how to protect yourself online as well as the different types of scams that are currently active.

- **CIFAS**
  www.cifas.org.uk

  CIFAS is the UK's leading fraud prevention service.

  For individuals they offer increased security against identity fraud, as well as expert advice on how to protect your personal data in our increasingly tech-reliant world.

- **Action fraud**
  www.actionfraud.police.uk

  This is the UK's national fraud and internet crime reporting centre. Action Fraud provides a central point of contact for information about fraud and financially motivated internet crime. Incidents reported to Action Fraud will be designated a police crime reference number.

Section 5
Current fraud trends

September 2020 – Amazon scams

There are 2 frequent scams – Amazon Prime subscription is due or a call from Amazon's fraud department to say your account has been hacked. They ask you to either download an app, click a link or request remote access of your computer to resolve issue.

Amazon state on their website that they will never call to ask you to install an app or ask for remote access.

See www.tsscot.co.uk/amazon-scams

July 2020 – COVID-19 scams

UK Finance have published details of the top 10 COVID-19 and lockdown scams the public should be on high alert for.

Further information can be found at www.ukfinance.org.uk/covid-19-press-releases/uk-finance-reveals-ten-covid-19-scams-the-public-should-be-on-high-alert-for