Fraud prevention guidance for clients

You, and your money, are targets of fraud.

Transactions between professionals and their clients are actively targeted by fraudsters, due to the large sums processed by the firm on behalf of clients.

This is particularly true of solicitors that conduct conveyancing transactions, debt recovery actions and estate administration (payment of beneficiaries) but can apply to any type of professional practice where client money may be held.

Peacock & Co work hard to ensure our fraud prevention processes and systems are secure and resilient to fraud. However, because fraudsters know that firms are a harder target, they move their attention to the 'client end' of transactions and may attempt to deceive you.

It is therefore vital that you maintain vigilance so that as a team we can ensure that information and funds are always secure.

As you have instructed us to act for you, it is important that you understand:

- what we do to help ensure that you do not become a victim of fraud; and
- your responsibilities to reduce the risks of fraud.

Further information on this, and some helpful tips on how to prevent fraud, may be found on the following pages.

Our commitment to you

We will ensure that we know you, our client

We undertake careful checks before taking on any piece of work, to ensure that you are who you say you are. For example, if you are selling a property, we will check that you own the property to ensure that we do not transfer sale proceeds to a fraudster.

When we send you money, we will check to ensure that we transfer funds to your account

We will always ask for your bank account details, either in a face-to-face meeting, or by hard copy letter sent by registered post. We can only make a payment to you as our named client, so please do not ask us to split monies across various accounts, pay other parties or beneficiaries etc. as we do not allow it and you will be able to do this quickly once monies are in your account.

We will provide our bank details at the start of the work, and will not advise you of changes by text message, email, via social media or by telephone

Our bank account details are provided to you once we have completed our initial onboarding checks at the start of the matter. We will only ever advise you of changes to our bank details by formal letter or in-person.

We will use secure methods of payment

This means CHAPS or BACS rather than immediate faster payments which are harder to recover if a fraud is later discovered.

We will take all reasonable steps to keep your data safe

We have strict policies and procedures in place to keep your data safe. We store your data on encrypted systems that are fully compliant with current data protection regulations. We follow rigorous procedures in data sharing with authorised counterparties.

We will keep our electronic systems secure and updated

We have professional-grade anti-malware solutions and secure email systems in place to help protect from ‘phishing’ and other cyber threats. We also have a policy of promptly installing relevant software updates and security patches on all work devices, including portable devices such as tablets and smart phones.

We will advise you of any known security breaches that may impact you

One of our lawyers, staff or partners specifically allocated to your work (as detailed in our client care letter will contact you to advise you of any known security breach that may affect you.

We will only email you regarding your case or transaction using a company email address using the domain peacock-law.co.uk.

Your security obligations

You will provide us with your best contact details

On or before the start of our work, we will ask for your contact details. You should use the same email address, telephone number/s, mailing address where-ever possible and anticipate further checks from us should you use other contact details in future.

You will communicate urgent instructions in person or by telephone

You should not rely on us receiving or reading your emails, particularly if you are providing time-critical instructions. We may request confirmation of your identity or other information.

You will never send us account details by email

We will not accept bank details via email. Ideally, you should send such details to us by registered post or come into our office personally. If you choose not to use these methods you do so at your own risk. We will however verify the bank details with you verbally in all cases and may ask you for documentary evidence of your bank details, such as a recent bank statement. Please be understanding should we need to double check anything that we think looks suspicious - this is for your security.

You will take all reasonable measures to keep your data and systems secure

You will keep your computer and mobile devices updated with the latest operating system updates, security patches, anti-malware solutions, and use MFA to protect your email account(s) and other online services.

You will inform us at the earliest opportunity if your email or devices become infected with a virus or other malware, or you think you've been hacked, scammed or your security is compromised.

Twelve key steps to prevent cyber fraud

1. Ensure that your PCs and other devices are protected behind an effective firewall, and up-to-date anti-malware and software updates are applied. Guidance at cyberaware.gov.uk/ is relevant for all to follow, to help protect your home and business from cyber-attack and fraud.

2. Try not to use public WiFi as you may be vulnerable to data interception. If you do need to use it to access email, online banking or make payments then use a VPN installed on the device.

3. If you use webmail for communicating with your professional advisors (solicitors, accountants, financial advisers etc.), then create a separate account for sharing information. Do not respond to any messages other than those from the professional you are dealing with. Confirm the legitimacy of other messages by phone. **Always check the sender's email address carefully.**

4. **Enable multi-factor authentication (MFA)** on email accounts and any other online accounts or apps where sensitive information is stored or accessed.

5. Create **strong, unique** passwords for each online service, especially email accounts. e.g. by using 3 random words (ideally including capital letters). E.g. *mountainFestivalpidgeon* or creating a memorable passphrase enhanced with a mix of letters, numbers and special characters, e.g. *5hopp!ng@Harr0ds*. The longer the words or phrase/sentence, the more secure it's likely to be. Where possible, use a **password manager** protected by MFA, for most of your accounts (but not your online banking accounts).

6. Never give out your usernames, passwords, or your one-time codes (from your Banking Security Token or mobile device) to anyone, no matter who they claim to be.

7. Pay little heed to unexpected emails. If your bank or solicitor (or anyone else legitimate) has something truly important to tell you (like they have detected fraud or need to verify your details) then they will contact you in a more reliable way - **they will not use text messages or email**. If you have concerns, call them using a telephone number from a reliable source (e.g. a printed bank statement or bank card will have phone numbers for your bank).

8. Exchange sensitive information with your professional advisor only once at the **outset of your instruction** or engagement, and ideally in-person. If you need to make a change then do so securely.

9. If you use online banking, then your bank will have included a message centre enabling you to send and receive messages securely. Only accept notifications and advisories from them using this method of communication; Do not act on telephone or email requests.

10. Be alert to social engineering and phishing emails or texts – **do not click on links or attachments** before verifying legitimacy of the email/links with the person separately.

11. Do not invite anyone to remotely connect to your computer for any purpose, including IT support or security help, unless you personally know and trust them. Unsolicited callers are always fraudsters.

12. Use ‘Block’ features available on your mobile phone and landline to blacklist any unsolicited callers or those who withhold their number. For example, in the UK the following service can be used: tpsonline.org.uk/.