Whitehead Monckton
the Kent law firm

Keeping you safe
Fraud Prevention Guidance for Clients

You, and your money, are targets of fraud. Transactions between professionals and their clients are currently being actively targeted by fraudsters, due to the large sums processed by us on your behalf. This is particularly true of lawyers 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.

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

*(i) what **we** do to help ensure that you do not become a victim of fraud*
*(ii) **your** responsibilities to reduce the risks of fraud.*

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 do 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 you with our bank details, and will not email you with changes
Our bank account details will be provided to you once we are in receipt of your ID. We will never advise you of changes to our bank details by telephone or by email.

We will use secure methods of payment
This invariably means CHAPS rather than immediate faster payments which are fairly impossible to freeze 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 the current Data Protection Regulations.

We will keep our electronic systems secure and up to date
We have professional-grade anti-virus and anti-malware software and firewalls 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 advisers or staff specifically allocated to your work (as detailed in our Client Care letter) will contact you by telephone or letter (not email) to advise you of any known security breach that may have compromised your information security.

We will only email you regarding your case or transaction *using the following company email address: firstnamesurname@whitehead-monckton.co.uk*

Your security obligations

You will provide us with best contact details
On or before the start of our work, we will ask for your contact details, and a preferred way of addressing you in communications. 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.

You will never send us account details by email
We will not accept bank details via email. You should send such details to us by registered post or come into our office personally. Please be understanding should we need to double-check anything that we think looks suspicious – this is for your benefit.

You will take all reasonable measures to keep your data and systems secure
You will keep your computer and relevant mobile devices updated with the latest operating system updates, security patches, and anti-virus software.

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, or your security otherwise 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-virus. 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 which are from the professional you are dealing with, including those purporting to be from their colleagues, without separately confirming by phone that such messages are legitimate. **Always check the sender's email address.**
4. Create **strong, unique** passwords, especially for your email account 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.
5. Use a **password manager** where possible, for most of your accounts (but not your online banking accounts). Use multi / two-factor authentication (MFA), and ensure that your password for your password manager is as strong as possible (e.g. enhancing the 3 random word approach with numbers and special characters, e.g. m0unta!nFestivalP!g3on.

   If you do not use a password manager, ensure you use MFA where possible, and a different strong password for each online service.
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 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 and ideally in-person. If you need to make a change then do so securely.
9. Validate calls from your professional advisor using a shared secret word or phrase, which you can establish with them at the outset of your instruction. Agree not to exchange the secret via email.
10. If you use online banking, then your Bank will have included a message centre enabling you to send & receive messages securely. Only accept notifications and advisories from them using this method of communication; **Do not act on telephone or email requests.**
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/