The Conveyancing Association Cyber Fraud and Fraud Protocol For England and Wales

The Conveyancing Association (CA) endorses the principles that underpin this protocol but recognises that each firm will have their own practices which may enhance the suggestions provided here or which, in combination, deliver the same or better standard of cyber security. Within these acknowledged limitations the CA commends the adoption of the protocol to its members as an opportunity to improve cyber security, manage the risks of fraud and protect both themselves and their clients from fraudsters.

This protocol is intended to deliver robust and efficient fraud prevention balanced between risk, profitability and the customer journey. Many of the suggestions also protect against Money Laundering or breaches of Data Privacy.

Whilst the item in italics are within the control of the business owner, all conveyancing teams should be aware of their importance.

Issue Addressed		Practice Guidance
1.0 Vishing **Vishing** is the act of using the telephone to scam the user into surrendering private information that will be used for identity theft.	A call from a fraudster attempting to collect confidential information or to facilitate the transfer of money to a fraudster's account.	Treat any call from anyone requesting confidential information with suspicion. Do not rely on caller ID which can be spoofed. Fraudsters will harvest information over time to make the call more believable so do not release information such as the name of your business relationship manager at your bank. If the call purports to be from your bank, ring your business relationship manager at your bank on a known phone number from a different phone so that the original caller is not still connected. If another phone is not available, ring someone you know first to check that the line is truly clear. Have a shared record of recognised contact details for your bank internally and keep this updated regularly. Do not transfer a caller to your nominated contact within your firm. Let that person know and ask them to call on their known numbers. Do not allow the caller to stop you ringing your known contact. Your bank will never request remote access to your computer and online banking or ask for your bank details.

1.1 Malware **Malware**, short for malicious software, is an umbrella term used to refer to a variety of forms of harmful or intrusive software, including computer viruses, worms.	A computer virus or Trojan is introduced to your computer to capture key-strokes and use them to access on line banking or other valuable personal data. Derived from 'malicious software', malware is any kind of software that can damage computer systems, networks or devices. Includes viruses, ransomware and trojans.	Indications of malware infection may include:- • Slow running systems • Unexpected pop-ups • System crashes • Running out of hard drive memory • Your contacts receive strange emails that appear to be from you • Unusual activity with programmes starting unexpectedly. To avoid being caught out:- *review the Actions to take section in the NCSC guidance on mitigating malware and ransomware attacks -* *https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks* • *Use up to date anti-malware as well as anti-virus software that scans email outside of your systems so that malware does not reach your internal networks* • *Maintain high quality security scans and update/update regularly* • *Scan all downloads whether from the internet, a USB or any other device* • *Only use approved software/applications which are actively approved before they are deployed on to devices* • *Separate system administrative accounts from user accounts to reduce the chance of privileges being exploited if a user account is hacked* • *Have separate individuals approve and send money transfers* • Log out of on-line banking when not in use • Remove card readers from your system when not in use • *If possible, dedicate a computer to banking, avoid using it for anything else (eg emails) and with an independent internet access* • *Ensure that your systems are backed up regularly, so should you be subject to an attack; enabling you to revert to the point before the malware infiltrated your system and reducing loss.*
1.2 Phishing **Phishing** is the attempt to obtain sensitive information such as usernames, passwords, and credit card details, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.	Emails pretending to be from a trusted source, encouraging the user to login to a duplicate website, or containing embedded malware, in order for the fraudster to record the keystrokes required to access your account.	• Treat any email asking you to login/register with suspicion, especially if misspelt or not addressed personally to you or how you would normally see emails from that company (do they normally just use your first name rather than first name & surname). • Always look at the email address, not just the name of the sender.

Whaling - type of fraud that targets high-profile end users such as corporate executives, company owners & board members, Politicians and celebrities**.** Suspicious emails can be forwarded to report@phishing.gov.uk which is a NCSC.GOV.UK service.		• Hover over links from emails to see what the true website address is. Your bank will not send you a link to a login page, only to their home page. • Do not use or click on links within emails, use the URL which you have always use, to log in. • *Avoid recording personal information on social media sites, this includes where you work, when you are away from home, where you eat.* • *Use spam filters to remove dubious emails.* • *Apply two factor authentication on systems or applications where available.* • *Review the NCSC Phishing guidance - https://www.ncsc.gov.uk/guidance/phishing.*
1.3 Smishing **SMS phishing** is a form of criminal activity using social engineering techniques. SPAM texts should be forwarded to **7726** (free) to report to your network provider	SMS text messages pretending to be from a trusted source requesting account details or giving instructions	• Remember: Your bank will never ask for account details by text, email or phone. • If from a client, check whether the mobile number matches the one you have for them on file. If in doubt, phone them from a trusted number.
1.4 Spear Phishing **Phishing** the attempt to obtain sensitive information such as usernames, passwords, and credit card details, for malicious reasons, by disguising as a trustworthy entity in an electronic communication. Spear phishing tends to be more targeted than phishing	Targeting potential high net worth individuals, intercepting emails to misdirect funds whilst they are known to be away from the office.	• Ensure that payments cannot be authorised without the proper payment requisition process being followed. • *Avoid posting on social media anything which would indicate that you are away from the office, especially if your social media account has been linked to your job/ role.*
1.5 Outbound Cheque Fraud https://www.financialfraudaction.org.uk/consumer/advice/cheque-fraud/	Law Firm cheques are stolen, altered or counterfeited	• Cross through spaces on cheques issued, after the payee name and amount. • If using a pen, use black or blue ink and press harder than normal to make it difficult to alter. If printing cheques, use a laser printer. • Use full names for the payee, rather than acronyms. • If a new cheque book does not arrive when ordered, report it immediately. • Keep cheque books locked away and do not sign cheques until you need them.
1.6 Inbound Cheque Fraud https://www.financialfraudaction.org.uk/consumer/advice/cheque-fraud/	Cheques are used to obtain funds or launder money	• Be suspicious of any cheque paid directly into your bank account without your knowledge. • Do not release funds before a cheque has been paid, as well as cleared, even if paid in 'by accident'. A 'cleared' cheque can still be unpaid. UK cheque clearing can take 6 days. There is no

		overseas cheque clearing system, foreign currency cheques are not payable into UK banks. • Do not accept a cheque for a higher amount that you were expecting.
1.7 Card Payment Fraud Credit card fraud is a term for theft and fraud committed using or involving payment cards as a fraudulent source of funds in a transaction.	Cards are intercepted or applied for using stolen documents	• Pay attention to card expiry dates and if your new card has not arrived report this to your bank immediately. • Cards can be collected from your local branch rather than posted. • *If you move premises, then advise your card issuer immediately.* • Shred all documents and cards before disposal. • Keep cards locked away.
2.0	Fraudsters posing as a client to defraud you	• Complete due diligence to identify all clients. • Check all signatures on ID documents against those on documents signed by your client. • Consider whether the circumstances of the client or the transaction raises suspicion.
2.1 Client Identity https://www.gov.uk/government/publications/proof-of-identity-checklist/proof-of-identity-checklist	Fraudster poses as a client to defraud a third party	• Complete due diligence. If you are not meeting the client, then consider asking for a selfie of them holding their ID document with the photo page open. Asking an estate agent or mortgage broker to do this can add an extra barrier to fraudsters. • If meeting the client, consider taking a picture of them holding their ID in your office to evidence that you are acting for the person identified. • Using electronic ID searches will identify if the ID document has been stolen and whether the official number on the ID is in the correct format. It will also identify the requirement for raised due diligence where the client is a politically exposed person, or on the sanctions list. • Do not be afraid to ask questions or for more evidence if there is any doubt.
3. Change of Bank Details https://actionfraud.police.uk/fraud-az-bank-account-fraud	Fraudster intercepts email to change bank details	• Where possible use a secure portal for all communication - most case management systems will have or support a secure portal. • Bear in mind that encrypted email will not protect against a recipient's email account being hacked which means that they could receive email from a fraudster. • Avoid sending or receiving bank details by email. Where possible, collect a client's bank details on your initial instructions form whether or not you expect to be making a payment to them. These details can also be used to return any leftover funds to enable the client account to be closed rather than having to rely on a client to cash a cheque. • Request a bank statement for the account to which they wish the payment sent so that you can ensure it is their own genuine account.

		• Where possible, provide the client with your bank details by post at the beginning of the transaction, advising them that these details will not change and they should ring the number on the letter to confirm any email purporting to be from your firm changing bank details. • Where there is a genuine change in bank details keep the existing bank account open until all transactions have been completed for clients notified of the original bank details rather than providing them with up to date details, so that you can tell clients when they instruct you that your bank details will not change during their transaction and they should ignore any communication implying that they have changed. • Collect a password, random memorable question and other identifying information from the client on instruction, such as their employment details, and store in your case management system so that you can verify that a call or email was initiated by the genuine client. • Require any party calling for an update to identify themselves so that you do not inadvertently tip a fraudster off as to when you will be requesting funds from your client or provide them with information which they could use to manipulate a client or someone else in your firm. • Consider using LawyerChecker, Lender Exchange or similar to verify account details. http://www.lawyerchecker.co.uk
4. Funds Recipient Identity	A funds recipient is created or cloned to defraud. This could be a client, Law Firm, estate agent, lender on redemption or anyone likely to receive monies from you	• Request Law Firm bank details with the contract pack so that they can be checked with account validation providers early in the transaction. • Check a Lender's redemption account details on the final redemption statement against those on the initial redemption statement. • Once successfully checked, hard code the bank details in your case management system so that payments cannot go to any other bank account without first being verified. • If a request to send funds to a new bank account arrives, ring the branch and speak to a Director or Partner to verify that they have changed their bank account. • Regularly review the SRA scam alerts page and subscribe to the RSS lead to view alerts as they are created. www.sra.org.uk/consumers/scam-alerts/scam-alerts.page
5. Caller Identity	Fraudsters ring to find out details about the transaction and to identify when payments may be sent	• All callers should be required to identify themselves and their relationship to the transaction. Ask them for information known only to someone genuinely related to the transaction.

6. Cyber Security	Prevent against a threat from a fraudster to your network	• Check that your internal systems are robust, especially if any are internet facing, using the government's self-assessment Cyber Essentials Checklist. Click here to access the checklist. *Cyber Essentials will help get a good baseline for your security system.* • Audit and test your systems regularly following NCSC guidance. • Complete the Cyber Essentials self-assessment but also work to obtaining Cyber Essentials Plus certification as the implementation of the 5 technical controls will improves cyber resilience. • For organisations that don't have sufficient expertise or capacity to do the work (apply controls etc.), try the Cyber Advisor scheme - https://www.ncsc.gov.uk/schemes/cyber-advisor/introduction • Also check out the Cyber Threat Report for the UK Legal Sector, which was published in June 2023 which has tips on defending against the various common attacks - https://www.ncsc.gov.uk/report/cyber-threat-report-uk-legal-sector
7. Cyber Security	Prevent against loss of data or infiltration of your network	• Implement a "bring your own device" policy so that any employees devices which connect to your system whilst they are at work or if you are allowing homeworking are adequately protected or excluded from your networks, following NCSC guidance. • Conduct penetration testing of your systems regularly to ensure that personal data of both clients and employees is protected. • Upgrade your fire wall and virus protection, installing updates as soon as they are released, known as patching. *See Cyber Essential & NCSC guidance.* • *The Small Business Guide has 5 steps and actions to take - https://www.ncsc.gov.uk/collection/small-business-guide*
8. Cyber Insurance	Many professional indemnity policies do not cover for cyber-attacks or loss of a Law Firm's own money through fraud	• Check whether your existing insurance covers for loss of the Law Firm's money and loss occurring as a result of a cyber-attack. • Consider taking out bespoke Cyber Insurance Policy if you are not covered through existing insurance. • Ensure your insurance cover meets your needs, are you still insured if your patching is not up to date? • Review NCSC cyber insurance guidance - https://www.ncsc.gov.uk/guidance/cyber-insurance-guidance

9. Prevention	Most Law Firm owners are aware of the risks but many employees are not	• Train all staff on the content of this protocol and the risks of cyber-crime. Try this free on-line course https://www.futurelearn.com/courses/introduction-to-cyber-security • Periodically test whether staff are complying with your policies e.g. mystery shop them to check whether they identify callers before giving out information. • Have robust joiner and leaver policies to educate joiners and remove access from leavers. • Encourage staff to check the actual email address as Outlook adds the person's name and this can be rigged. Fraudsters also use default fonts to create false emails which look the same eg lower case "L" and capital "i" • Where possible record calls and random sample them to ensure process is being adhered to. • Make sure that employees being contacted by banks etc. understand who the correct contacts are and do not give out information if prompted. • Make staff aware that Vishing, Malware and Phishing are an ongoing process. Fraudsters will ring or email to obtain information to enable them to ring back pretending to be someone else. Having harvested sufficient information they socially engineer the firm into installing Malware so they can see the progress in the transaction and the moment to Phish; sending instructions to redirect monies to their own account. It is therefore vital that staff do not give out information, without identifying that a caller is genuine. • Regularly check Rules and Alerts in your email exchange to check for Rules which identify emails with funds requests in them and forward them to fraudsters who then attempt to mis direct the funds. • Check anyone with access to the office. Files should be locked away and any rubbish indicating progress or bank details shredded. Protect scanners, copiers and printers with a PIN, they have hard drives in them which can be programmed to record information. • Where possible, provide staff with access to a Virtual Private Network if they are going to be working from home or on the go. Do not promote the use of public wi-fi from internet café's, hotels etc, it is generally unsecure. Consider using wi-fi dongles, so public wi-fi does not have to be used. • Have a documented recovery plan in hard copy in case of a malware attack. Include contact numbers and actions in the event of an attack.

		• Buy all versions of your website address to avoid fraudsters setting up a plausible cloned website to pose as your business. • Include in your terms of business the client's informed authority for you to report a fraud to Action Fraud. Sign up for National Cyber Security Centre (NCSC) Early Warning System
10. Actions when funds have been fraudulently redirected	Legal requirements and those which might reduce loss if completed quickly	• You and your client should immediately contact the recipient bank and ask them to freeze the account to prevent the money moving any further. The bank will move it to their fraud ledger, pending investigation. • The client should contact their bank and ask them to contact the receiving bank and request the return of the monies. • You must complete an Action Fraud report online at www.actionfraud.police.uk and call the National Fraud and Cyber Crime Reporting Centre on 0300 123 2040. • Your Money Laundering Reporting Officer should send a Suspicious Activity Report to the National Crime Agency concerning the movement of funds to a criminal's account. • Advise your Regulator.