JTC

STRONGER TOGETHER

CLIENT GUIDE: CYBER FRAUD AWARENESS

PROTECTING YOURSELF FROM FRAUD

PROTECTING YOURSELF FROM FRAUD

JTC Group operates a range of measures designed to protect itself from fraud including criminality arising from cyber-attacks. However we also recognise the importance of helping to ensure that our valued clients also protect themselves from the ever increasing threat of malicious parties attacking systems to perpetrate fraud. Such actions often involve identity theft and the guidance contained in this document is designed to assist our clients in the prevention and identification of fraud attempts.

The following information seeks to identify common categories of fraud and offers some practical guidance that can be adopted by individuals and/or corporate entities to assist in the prevention or early identification of fraud.

If you suspect that you are subject to a fraud attack it is critical that you act quickly. It is possible that your usual email communication channels with JTC have been compromised and therefore upon suspicion of fraud it is important to ensure that you immediately telephone a known JTC contact to raise any concerns and to seek guidance.

ISSUE	DESCRIPTION	PRACTICAL GUIDANCE
VISHING	Is the act of using the telephone to scam the user into surrendering private information that will be used for identity theft e.g. receiving 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. Do not release information such as the name of your relationship manager at your bank. › If the call purports to be from your bank, inform the caller that you will ring your bank. Then proceed to call the bank on a known phone number. › Create and maintain a record of recognised contact details for your bank. › 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.
MALWARE	Short name for malicious software. It is an umbrella term used to refer to a variety of forms of harmful or intrusive software, including computer viruses, ransomware, Trojans, logic bombs and worms.	› Slow running systems › Unexpected pop-ups › System crashes › Running out of hard drive space or memory › Capturing of keystrokes › Encrypted files and ransoms for payment › Your contacts receive strange emails from you › Unusual activity with programmes starting unexpectedly To avoid being caught out:- › Use up to date anti-malware software that scans email outside of your systems so that malware does not reach your internal networks › Maintain high quality security scans and 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 (e.g. emails) and with 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.

ISSUE	DESCRIPTION	PRACTICAL GUIDANCE
PHISHING	Phishing: typically received via email. These emails pretend to be from a trusted source, encouraging the recipient to open a malicious attachment or click on a link in an attempt to obtain sensitive information such as usernames, passwords and credit card details, often for malicious reasons. Whaling is a type of fraud that targets high-profile end users such as corporate executives, company owners & board members, politicians and celebrities.	› Use spam filters to remove dubious emails. › Always look at the email address, not just the name of the sender. › 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). › Do not use or click on links within emails, use the URL which you always use, to log in. › 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. › Avoid recording personal information on social media sites, this includes where you work, when you are away from home, where you eat. › Apply two factor authentication on systems or applications where available. › Ensure that payments cannot be authorised without the proper payment requisition process being followed.
SMISHING	SMS phishing is a form of criminal activity using social engineering techniques by 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. › Your network provider may offer a service for these SPAM texts to be reported.
OUTBOUND CHEQUE FRAUD	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 expected after being ordered, report it immediately. › Keep cheque books locked away and do not sign cheques until you need them.
INBOUND 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.
PAYMENT FRAUD	Payment Fraud is a term for theft and fraud committed using a payment solution I.E. cards or electronic payment solutions such as PayPal, as a fraudulent source of funds in a transaction.	› Cards can be 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 received through your postal system. › If you move premises, then temporary reroute all post until you have updated your address on file to all senders. › Shred all documents and cards before disposal. › Keep cards locked away.

ISSUE	DESCRIPTION	PRACTICAL GUIDANCE
IDENTITY THEFT FRAUD	Fraudsters posing as a client to defraud you or a third party.	› Complete due diligence to identify all clients. If you are not meeting the client face-to-face, then consider additional ID verification processes. › 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 a sanctions list. › 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. Do not be afraid to ask questions or for more evidence if there is any doubt.
CHANGE OF BANK DETAILS	Fraudsters intercepts email(s) and requests changes to bank details.	› Where possible use a secure portal for all communication exchanges. › 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 alone particularly where new banking instructions are being communicated. › Where possible, provide your banking details by post (or other secure means) at the beginning of a transaction, advising your counterparty that these details will not change and they should ring the number on the letter to confirm any email purporting to be from you requesting any changes to bank details. › Establish clear written operating protocols with counterparties who process payment instructions for you that are designed to authentic instructions.
FUNDS RECIPIENT IDENTITY	A funds recipient is created or cloned to defraud.	› Establish direct contact with genuine funds recipient, authenticate their identity and seek written confirmation of funds payee details.
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 multiple pieces of information known only to someone genuinely related to the transaction.

Below are a number of recommended practical guidance tips professional and private clients may seek to implement. The list is not exhaustive, and any client may seek to obtain independent Information/Cyber Security advice to fully assess and determine the necessary controls to implement, applicable to their environment.

BEST PRACTICE	DESCRIPTION	PRACTICAL GUIDANCE
CYBER SECURITY	Identify	› Implement an established and suitable Information Security risk governance and framework structure. › Companies should create and implement the necessary and applicable Information/Cyber Security Policies, documenting the control requirements applicable to their business. › Companies should perform assessments on their infrastructure, applications, cloud, staff and other internal systems to ensure compliance with policies and environment(s) are robust for their needs and service offerings and implement the necessary controls required. › Perform the necessary assessments on your supply chain/service providers and applications regularly. › Ensure risks are identified, documented and there is transparency to applicable stakeholders and agree the required risk treatment plan.
CYBER SECURITY	Protect	› Deploy the required perimeter security controls I.E Email, Internet and physical. › Strategically deploy, monitor and manage Firewalls across your environment. › Ensure all systems and application devices have the latest stable security patches installed. › Where possible perform automated patch management. If automation is not possible, patching should be performed on a regular basis. › Conduct penetration testing of your systems regularly to identify potential vulnerabilities and mitigate. › 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 cafes, hotels etc, it is generally unsecure. Consider using Wi-Fi dongles, so public Wi-Fi does not have to be used. › Where possible implement multifactor authentication for log-in and payment systems. › Set a secure, strong and complex password and access control policies. › Store passwords securely in a password vault/safe. › Check anyone with access to office premises. Files should be locked away and any unwanted printed data should be shredded. Protect scanners, copiers and printers from random access. › Buy all versions of your website address to avoid fraudsters setting up a plausible cloned website to pose as your business. › Develop and deploy a suitable Security Awareness program. › Educate your staff and yourself on the risks of cyber-crime and how to protect yourself. › Be sceptical about links and attachments in emails. › 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. › Avoid sharing personal information over social media. › Avoid accessing personal and financial information over public Wi-Fi. › Make sure that your employees being contacted by banks etc. understand who the correct contacts are and do not give out information if prompted.

BEST PRACTICE	DESCRIPTION	PRACTICAL GUIDANCE
CYBER SECURITY	Detect	› Deploy an event management and monitoring solution, that can help triage events and distribute alerts when required. › Utilise a Security Operations Centre (SOC) solution.
CYBER SECURITY	Respond	› Create the necessary Incident Response Plans, review, update and test regularly. › Deploy an intrusion detection prevention and response solution that can help contain and isolate machines in the event of an incident.
CYBER SECURITY	Recovery	› Consider whether your insurance cover may be prudent or if existing coverage is adequate. › Ensure the necessary Business Continuity and Disaster plans are documented, reviewed, updated and tested regularly. › Ensure these plans are accessible to the required staff in the event of a recovery. › Perform regular encrypted backups to help aid recovery.
ACTIONS IF FUNDS HAVE BEEN FOUND TO BE FRAUDULENTLY MIS-DIRECTED	Actions that may reduce loss if completed quickly	› Perform a thorough incident analysis and investigation to determine the full scale of the incident and take the necessary actions to contain, eradicate, preserve evidence and recover. › Be aware that IT systems (including email communications) may be compromised so any notifications to counterparties and banks should be through secured channels. › You should immediately arrange for the relevant banks to be contacted to recall the funds on the basis of a fraud and to prevent any further activity over the account without additional security measures. › If the identified fraud relates to your relationship with JTC, you should securely notify a JTC contact as soon as possible for assistance and guidance.

IMPORTANT NOTE:

The information in this document provides some practical guidance on security controls which could help prevent individuals or corporate entities falling victim to fraud and includes industry best practices, methods and tips but it remains the responsibility of everyone involved to remain vigilant to ensure that the fraudsters do not achieve their aims.

Remember: If you suspect that you are subject to a fraud attack, it is critical that you act quickly.

It is possible that your usual email communication channels with JTC may have been compromised and so upon suspicion of fraud, it is important to ensure that you immediately telephone a known JTC contact to raise any concerns and to seek guidance.