Protecting your business from some of the current fraud threats

This literature provides guidance on fraud prevention and is provided for information purposes only. Where noted the guidance provided has been sourced from third parties.
The Annual Fraud Indicator published in 2013 by the Home Office, estimates that Fraud will cost the UK economy £52bn.

Some of the current threats we are seeing are:

• Payment fraud
• Cheque fraud
• Internal fraud
• External fraud
• Online safety
Payment fraud

Standing Order Fraud

- There has been a small increase in Standing Order Fraud with multiple attempts by criminals to set up mandates on corporate client accounts
- Compromise can come from the interception of legitimate cheques in the post. Cheques are a favourite route as a completed cheque will contain the account details and the signatures of the client
- Once a victim account has been identified by criminals they normally flood the system with multiple attempts. This is to test the banks’ systems and controls in the hope that, out of a number of attempts, at least one will be successful and funds will be paid out.

Action
In Standing Order Fraud, the key to reducing attacks is to remain vigilant and prevent any successful debits. This will drive the criminals elsewhere as they will not continue to attack an account where they are not getting a return.

Invoice Fraud

- Fraudsters are pocketing millions of pounds through invoice fraud each year, directly targeting clients across all sectors, regardless of industry or size
- This type of fraud involves a communication sent to the client by the fraudster, purporting to be from their genuine client or supplier. The communication provides a change of bank details to be used for future payments
- A subsequent payment, which is often upwards of hundreds of thousands of pounds, is then made to the fraudster’s account and it is only when the genuine beneficiary contacts our client for non-receipt that the fraud is identified.

Action
The Fraud Warning on the next page has been issued by the Barclays Fraud team and incorporates a National Fraud Intelligence Bureau (NFIB) alert. This provides information and preventative guidance to help combat invoice/ BACS divert fraud.
Payment fraud

Fraud Warning
Have you been asked to change the bank details for a client/supplier? This may be an attempt to defraud you. Invoice Fraud involves clients receiving requests, purporting to be from genuine clients or suppliers, which direct them to change the bank details used for electronic payments. Losses in the UK to date are reported to be over £150 million. If you believe you are a victim, please report this to Action Fraud at www.actionfraud.police.uk or call 0300 123 2040.

The key signs of invoice fraud are:
• The counterfeit invoices and any covering letter may be printed on a scanned copy of the company headed paper; consequently, the company logo may appear somewhat blurred
• Contact details may differ from that provided previously, e.g. the email address may end in ‘.org’ or ‘.co.uk’.

Some examples of how to reduce the risks:
• Always confirm any request to change bank details with your usual contact, before effecting the change
• Instruct staff with responsibility for paying invoices to check invoices for irregularities and escalate suspicions using a known contact
• Consider setting up designated ‘Single Points of Contact’ with companies to which you make regular payments
• Consider reviewing previous requests to change account details to confirm they were genuine
• Consider contacting your clients to alert them to this type of fraud, to prevent your clients acting on an instruction purporting to be from you and transferring money owed to you to a fraudster.

Please remember that electronic payments in the UK are made based on the sort code and account number only. Any account name given is not routinely checked as part of the automated payment process. This is the same for all UK banks. It is the responsibility of the remitter to ensure the account details being used are correct, by conducting independent verification.

More information on the payments system and other consumer guidance can be located at www.fca.org.uk. General fraud prevention advice on other types of fraud can be found on the Action Fraud website: www.actionfraud.police.uk.
Cheque fraud

Additional payee added
Cheque fraud focus has moved to an increase in cheques with an addition to the payee line, thus removing the need for the fraudster to alter the existing details on the cheque. These are harder to detect when there is no alteration – just an addition – as the cheque has not been ‘washed’.

Action
• When completing cheques, it is best practice to draw a line through all unused space on the payee line and, if possible, include the payee account number
• For more detailed information, read the Best Practice Guidelines for Business Users of Cheques, issued by the Cheque and Credit Clearing Company (C&CCC) at www.chequeandcredit.co.uk.

Overpayment/Refund Fraud
This type of fraud is typically seen when a cheque is deposited to an account for in excess of a recently received order for a new client or has been credited unexpectedly. Clients will then be asked to refund all or part of the overpayment. The reason given for this may be that whoever has placed the order has sent too much money to the client or that the order is no longer required. Urgency is usually stressed in these types of situations and either way when the cheque bounces, clients will be left with a loss.
Fraudsters may also attempt to involve clients in moving fraudulent funds and this will be where clients receive funds electronically and again are asked to refund all or part of these funds to an account. In this situation, someone else may have been defrauded and clients are being asked to unknowingly assist in moving these funds.

Action
• You should exercise caution if asked to make refunds, particularly if the person or business asking to do this is new or previously unknown
• If you are unsure if the item appearing in their account is cleared or not, contact the bank and confirm this
• If you are in any way concerned about the request, decline to make the refund until entirely happy. Contact the bank if you think you may have been defrauded in this way.
Cheque fraud

Compromised/Stolen Cheques

- Original cheques are usually compromised when they are posted out by legitimate clients and the point of compromise can be at anywhere from between the Barclays client’s mailroom to the beneficiaries’ mail room/post box.

- This type of fraud sees criminals stealing cheques and, rather than altering them, opening accounts in the payee name on the cheque. For example, if a cheque has been made out to HSBC, a criminal will open an account in the name Harry Simon Brian Charles T/AS HSBC. There are no restrictions on T/AS account names, although reasonable checks are carried out when these accounts are opened.

Action

- Do not leave mail unattended in mail rooms overnight as items could be stolen at this point. It is also good practice to vary the packaging in which cheques are despatched to help prevent compromise in the postal systems. Window envelopes should be avoided as these are far easier for criminals to identify in mail rooms.

- If you do need to use cheques, it is recommended that the value of these cheques are kept to a minimum as the higher value cheques are often more attractive to fraudsters in this type of fraud.
Internal fraud

Controls
This continues to be an area where our clients can be vulnerable. Mainly where controls are not operated or controls have not been reviewed end-to-end. This can lead to abuse of the process by staff. Not all firms have a fraud-specific control during employment screening. Some firms do not have two to sign off their payment processes.

Action
• Processes – centralise where appropriate to enable consistency of control
• Controls – design appropriate controls that fit into the key process points
• Test that controls are operating as expected
• Monitor fraud and operational losses and attempts
• Monitor risk events including where losses have not been noted
• Post-event deep dives enable continuous learning
• Your auditors should be able to provide advice on all these points
• Two to authorise on separate machines
• Secure networks
• Securing authentication devices and passwords
• Authentication, Authorisation and Accuracy.
Internal fraud

Procurement Fraud – the risks
• Employees spending company money for private gain. For example, paying for non-existent services
• ID passes, passwords and private information being stolen by dishonest contractors and tradesmen.

Action
• Reconcile bank statements and company credit card statements meticulously and regularly
• Encourage employees, clients, suppliers and business partners to report anything unusual
• Set guidelines and processes for who can place orders on behalf of the company. Use a formal purchase order system
• Take up references for, and consider vetting new employees and contractors
• Respond to payment card chargeback requests promptly
• Set strict credit limits
• For information on Staff Policies and what you could include in an Acceptable Usage Policy, visit: www.getsafeonline.org/businesses
External fraud

The Risks

• Fraudsters targeting your telephone system to make calls to premium rate/international numbers
• Fraudsters setting up a merchant account in your company’s name and accepting orders for goods that they do not supply
• Fraudsters hijacking your website to redirect orders to their server
• Fraudsters posing as company directors, then changing the directors and registered address of the business
• Goods being ordered with bogus account details or stolen credit cards
• Payment card chargebacks as a result of clients fraudulently claiming that goods have been received not fit for purpose or not received at all.

Action

• Restrict destinations on your telephone systems that would not normally be dialled (e.g. premium rate/international) and ensure that it is not possible to access voicemail systems from outside lines. More details can be found at: www.actionfraud.police.uk
• Be aware of registration of new domains that are similar to yours. Consider registering common mis-spellings and variations of your company name
• Perform credit checks on new clients and check their contact details for authenticity
• For unknown clients with no transaction history, insist on cleared payment being received before goods or services are supplied
• Perform credit checks on new suppliers and partners, and check their contact details for authenticity
• If selling online, validate new clients using verification such as Address Verification Service, or Verified by Visa / MasterCard SecureCode. There are a number of commercial providers of verification solutions and details that can be found via www.cardwatch.org.uk
Social Engineering and Cyber Fraud

The Risks

• Social engineering is the manipulation of situations and people that results in the targeted individuals divulging confidential information.
• Scam emails and pop ups are designed so that the victim unknowingly downloads malicious software (malware) programs which can infiltrate, corrupt and steal information from computer systems, such as the company’s online banking details.

Action

• Think about social media networks and your website – it is vital that personal details such as date of birth or employment information are not readily available for fraudsters to use.
• Avoid sharing the movements of senior staff on social networks or your website – this may seem harmless but can help fraudsters to use this information to impersonate them.
• Do not click on links or attachments or respond with personal information to unsolicited emails or text messages even if appearing to be from a known sender such as Barclays; always access sites through known and verified links or go to the company’s website using an internet browser.
• Be cautious of unusual requests from a known individual/organisation, such as a payment to a new account; a change of bank details, or a request for personal details. Do not respond and contact them independently to verify any request. If their computer has been infected with malware; the email may not have been sent by them.
• Don’t respond to unsolicited phone calls even if the caller appears to have relevant information about you or the business. Always call back from a different phone to a number from the company’s legitimate website, not the number you received the call from.
• Be wary of clicking on pop up messages claiming your machine is infected or asking you to click on an image or text, as it could actually be malicious software that allows the fraudster to remotely access and control your computer.
• Always challenge giving out personal or financial details to anyone.
• Keep up to date with the latest social engineering techniques and malware threats and how to protect your business against these and many other problems encountered online, by visiting www.getsafeonline.org.
Social Engineering and Cyber Fraud

• Ensure that all sensitive information and files are backed up on external devices disconnected from a network or the internet.
• Install and regularly update anti-virus/anti-spyware software on all systems and ensure firewall settings are up to date and set to the highest protection level. Use strong passwords including upper and lowercase letters; numbers and special characters.
• Consider using a dedicated computer for your payment transactions, with a separate computer for emails/ general internet browsing, reducing the risk of exposure to malware.
• The National Crime Agency (NCA) provide information on their website on how to identify viruses and if identified, how to clean your computer.
• Users who have the authority to view account information and make payments should keep their smart card secure at all times in the same way as their debit or credit card. Once used, remove the smart card from the card reader (even while still logged in) when not being used to sign a payment or perform an administration change.
• They should always log out from payment systems, remove the smart card and store it securely. Smart cards should never be shared.
• They should memorise their PIN and not disclose this to anyone. This includes not allowing the web browser to remember details of the PIN.
• Use dual authorisation where possible. For example one staff member can input payments on a machine and then a second staff member should check these before authorising on another machine. Reconciliation should be carried out regularly.
• Raise awareness amongst your staff, customers and suppliers.

Reporting Fraud

Action Fraud is the UK’s national fraud reporting centre where you should report fraud if you have been scammed or defrauded. The service is run by the City of London Police working alongside the National Fraud Intelligence Bureau who are responsible for assessment of the reports and to ensure that your fraud reports reach the right place. The City of London Police is the national policing lead for economic crime.

You can report fraud online or by calling 0300 123 2040.