Bank Mandate Fraud

Guidance Document

Business or public, we are all at risk of bank mandate fraud

nafn gov.uk Data & Intelligence Services

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

First Release **July 2018**

Bank Mandate Fraud Guidance

Introduction

This guide aims to provide an awareness of bank mandate fraud, reinforcing this through real life case studies and followed by useful prevention advice.

Definition

Bank Mandate fraud occurs when someone requests you to change the bank transfer mandate, by purporting to represent an organisation you make regular payments to, for example business supplier, membership or subscription.

Fraudsters will look to identify suppliers of services you or your organisation use on a regular basis. This can be obtained from details of contracts awarded or other information which is published on websites in line with transparency.

The payment is made as requested and the fraud is complete.

SERIOUS
Organised Crime

Serious Organised Crime groups are profiting from fraudulent schemes that target organisations and individuals.

Bank mandate fraud is frequently used by these groups as it carries low risk and potentially high rewards.

RISKS

Bank mandate fraud is constantly evolving and can be cyber enabled. In all cases the victim, either a person or organisation will lose money that is unlikely to be recovered.

Public Sector organisations' are particularly at risk due to the high volume of transactions and the opportunity to obtain a significant sum of money in just one transaction.

Examples of Bank Mandate Fraud

1. **Your online bank account** is hacked into by a fraudster and monthly payment details are altered so that the money is transferred to the fraudsters account.

2. **You are contacted by someone** pretending to be from an organisation you have a standing order with and request you change the order to reflect a change in their banking. The standing order mandate is changed accordingly but next month the actual organisation fails to deliver your products or a membership has been cancelled as they did not receive their payment.

3. **As a business you are contacted by someone** pretending to be one of your suppliers who inform you they have changed their bank and request a change to an existing direct debit. As a result the bank mandate is amended to the fraudsters account provided. The next month you are contacted by your genuine supplier asking what has happened with the monthly payment.

Real Life Case Studies (anonymised)

Local Authority example - A local authority had numerous construction contractors for the refurbishment of schools. The local authority received an apparently genuine letter from one of these contractors stating they had changed their banking details. No checks were conducted and the bank details were updated. Within a week two payments totaling over 2 million pounds were transferred to a bogus bank account. The fraud was complete and funded Serious Organised Crime.

Charity example - An accountant at a charity received a phone call from a male purporting to be from a high street bank. The fraudster's number was 'spoofed' to resemble the banks phone number and the caller stated there had been attempts by a third party to access their account. The fraudster spent considerable time gaining the confidence of the accountant, even sending them a plausible email that looked like it had come from the bank. The fraudster persuaded the accountant to download 'team viewer', which allowed the fraudster remote access to the charity's bank accounts.

The accountant was convinced to provide log in details for a second bank account. The fraudster told the accountant that both accounts would be subject to "ghost transactions" to test their security and the money would not actually leave the accounts. However, this was a lie and a six figure sum was transferred to numerous fraudulent accounts. The fraud was complete and funded Serious Organised Crime.

Sports organisation example - A private sector sport organisation were re-developing their building. They received an email with an attachment purportedly from the construction company. A Trojan virus was unknowingly downloaded via malware which allowed the fraudster remote back door access to all email traffic. Shortly thereafter an email was received from the fraudster pretending to be from the construction company informing them of a change of bank mandate details and a reminder of an upcoming payment. A six figure sum was thereafter paid to the fraudster's account. The fraud was complete and funded Serious Organised Crime.

The Do's and Don'ts

The cost of fraud is at record levels, is often difficult to detect and can be expensive to investigate. Organisations successful in reducing fraud have done so by focusing on pre-empting it through establishing stronger anti-fraud cultures.

It's important to implement and maintain robust processes around fraud prevention and make it part of your "business as usual" activities including who and when to report incidents of attempted fraud.

DO's

1. Check it twice or pay the price! Carefully check the senders email address to identify if it exactly matches with your known records.
2. Know your top 20 creditors! Mandate fraud is more likely to be perpetrated against a major organisation be alert to any requests to alter their bank details.
3. Make an 'Open Source' check on the internet of the new bank account sort code and account details to uncover:
   a. Location of the bank and check against the location of the company, and
   b. Whether there are any blogs or information available to suggest the communication is a scam.
4. Validate all requests for bank account changes using established contact details. Never use any of the contact details contained within letters/emails received; whilst many email addresses appear genuine often there is a minor change. If you are concerned about the source of a call ask them to provide you with a switchboard number or hang up and call them back using an established contact number.
5. Enquire over the veracity of the change of bank account details. If the change appears genuine, request that the supplier repeats the request but with details of the previous AND the new bank account details referenced.
6. Adopt dual control procedures for authorising payments. Have a senior member of the finance team to review your activity and if satisfied to authorise the change of bank account details.
7. Regularly reconcile your bank statements and report anything suspicious to your bank immediately.
8. If the communication is deemed to be a scam - consider sharing this information as an 'Alert' with the National Anti-Fraud Network (NAFN) who will notify other partner groups who may also be affected.

DON'Ts

1. Don't leave sensitive files like bills lying around. Visitors could look at and record details of standing orders and direct debits.
2. Don't give out sensitive information over the phone, via email or in person to anyone that you are unsure of. Fraudsters will piece together snippets of information from different sources to allow them to commit fraud. This is known as 'Elicitation.'
3. Don't feel pressured to disclose information. Bank Mandate Frauds are often accompanied by routine conversation followed by a 'switch in tempo' and an urgent request. Nothing is so time critical that it can't wait until you have verified who you are dealing with.

Practical Scenario

A Public Sector Organisation has a long standing contract with a local construction company called 'Construction Solutions Ltd.'

The Public Sector Organisation receives an email from Roddy Smith, the finance manager of 'Construction Solutions Ltd. Roddy advises that their bank account details and sort code have changed. Enclosed is the latest invoice for £252,383.66, requesting payment before the end of the week as they have cash flow issues.

The email is received by Angela Brown from Public Sector Organisation accounts, who has regular communication with Roddy Smith. He is a 'nice guy' to work with. She is inclined to make a quick adjustment as requested, however the Public Sector Organisation Finance team have recently reviewed and updated their Serious Organised Crime Prevention processes. This includes significant changes to the process for making payments to suppliers who intimate changes to bank account details.

STOP & THINK!

Angela is aware of the new process. She thinks it is quite convoluted but she complies with this as outlined in the 'Do's and Don'ts'.

Through Angela making checks outlined in their new Serious Organised Crime Prevention processes, it was established that the email from 'Roddy Smith' at 'Construction Solutions Ltd' was fraudulent. By following the amended process, the Public Sector organisation avoided making a payment of £252,383.66, to a Serious Organised Crime group actively involved in bank mandate fraud activity.

Conclusion

The drive towards transparency, improved online information and poor social media security all provide fraudsters with information that enables them to assume false identities to conduct bank mandate fraud. By recognising the tactics used by fraudsters, organisations can protect themselves against bank mandate fraud by adopting these procedures as part of their fraud prevention resilience culture.

Remember...
Once the money is gone it is very unlikely that it will be recovered!

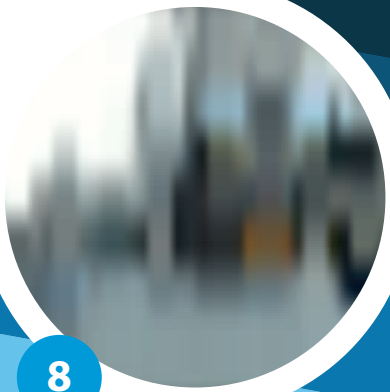
Additional Advice

Malware
Malware is a general term for malicious software. Malware includes viruses, worms, Trojans and spyware.

Trojan
A backdoor Trojan allows someone to take control of a user's computer without their permission.

Spoofing
Spoofing, in general, is a fraudulent or malicious practice in which communication is sent from an unknown source disguised as a source known to the receiver.

Team Viewer
TeamViewer is proprietary computer software for remote control, desktop sharing, online gaming, web conferencing and file transfer between computers.



Police Scotland:
www.scotland.police.uk/contact-us/report-fraud

In Scotland all reports of fraud and any other financial crime should be reported to Police Scotland by calling 101 without delay.

Take 5:
takefive-stopfraud.org.uk/advice/

Action Fraud:
www.actionfraud.police.uk/mandate-fraud
In England, Wales and Northern Ireland if you have been a victim of fraud or cyber crime, report it to Action Fraud at **actionfraud.police.uk** or by calling 0300 123 2040

Get Safe Online:
www.getsafeonline.org/ways-you-work/mandate-fraud/

nafn gov.uk Data & Intelligence Services

National Anti-Fraud Network:
www.nafn.gov.uk
The National Anti-Fraud Network, NAFN Data and Intelligence Services provide a range of services to support the work of local and public authorities throughout the United Kingdom. NAFN is widely recognised as a provider of data and intelligence to local government, housing associations, NHS and wider public authorities.

If you would like to become a member of NAFN or learn more about its services email **general@nafn.gov.uk**

POLICE SCOTLAND
Keeping people safe
POILEAS ALBA

ActionFraud
National Fraud & Cyber Crime Reporting Centre
actionfraud.police.uk