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 practical advice on fraud prevention.

Definition

Bank Mandate fraud occurs when an unauthorised request is made to change the details of a bank transfer mandate. Fraudsters may access your bank account and change the details or claim they are a genuine business supplier to your organisation.

Fraudsters will look to identify suppliers of services that 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.

If the payment is made as requested, 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 most cases the victim 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 a single 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 fraudster's account.

2. **You are contacted by someone** pretending to be from an organisation you have a standing order with and they request that 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 due to the amendments made the payment went to the frauster.

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

Real Life Case Studies

Local Authority example - A local authority had numerous construction contractors for the refurbishment of schools. They 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 were transferred to a bogus bank account.

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 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.

Sports organisation example - A private sector sport company was undertaking building improvements. 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 after an email was received from the fraudster pretending to be from the construction company informing them of a change of bank mandate details with a reminder of an upcoming payment. A six figure sum was mistakenly paid to the fraudster's account.

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 treat it as a "business as usual" activity. You need to be clear about when and where to report all incidents of attempted fraud.

DO's

1. Check it twice or pay the price! Carefully check the sender's email address to identify if it exactly matches your known and trusted 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 (to be checked against the company address) and
   b. Whether there are any blogs or reports available to indicate 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, contact the company directly using a known and trusted email address or telephone number.
5. Adopt dual control procedures for authorising payments. Ensure that a senior member of your finance team reviews your actions and formally authorises the change of bank account details.
6. Regularly reconcile your bank statements and report anything suspicious to your bank immediately.
7. If the communication is deemed to be a scam, consider sharing this information with Police Scotland, Action Fraud and the National Anti-Fraud Network (NAFN) who will issue an alert notifying other organisations that may also be affected.
8. Regularly review and update your security policies ensuring that all staff are fully briefed and trained to spot potential fraud.
9. All attempted fraud, whether successful or not, should be reported to one or more of the organisations listed on the back page of this document.

DON'Ts

1. Do not leave sensitive files like bills lying around. Visitors could look at and record details of standing orders and direct debits.
2. Do not 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 conversations followed by a 'switch in tempo' and an urgent request. Nothing is so time critical that it cannot wait until you have verified who you are dealing with.
4. Do not use social media to disclose business arrangements, personal contacts and working relationships. Fraudsters may use such information to appear genuine.

Good Practice Example

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

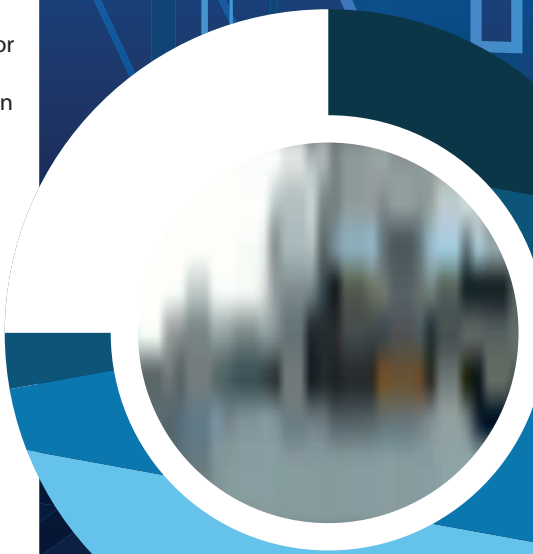
The Public Sector Organisation receives an email from Roddy Smith, the finance manager of Construction Solutions Ltd. Roddy advises that their bank account details and sort code have changed. Enclosed is the latest invoice for £252,383.66 with a request forpayment before the end of the week to help with 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 has recently reviewed and updated its Serious Organised Crime Prevention processes. This includes significant changes to the process for making payments to suppliers who submit changes to bank account details.

Angela is aware of the new process. She thinks it is quite convoluted but she follows the advice outlined in the 'Do's and Don'ts' set out in this document.

Angela's checks and close scrutiny established that the email from Roddy Smith at Construction Solutions Ltd was fraudulent. Adhering to good practice prevented the Public Sector Organisation from making a payment of £252,383.66, to a Serious Organised Crime group actively involved in bank mandate fraud activity.

Stop and Think!



Conclusion

The drive towards transparency, improved online information and poor social media security provide fraudsters with details which enables them to assume false identities to conduct bank mandate fraud. By recognising the tactics used by fraudsters you can protect yourself against bank mandate fraud. All individuals and organsations should acknowledge the risks and adopt a fraud prevention resilience culture.

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

Additional Advice

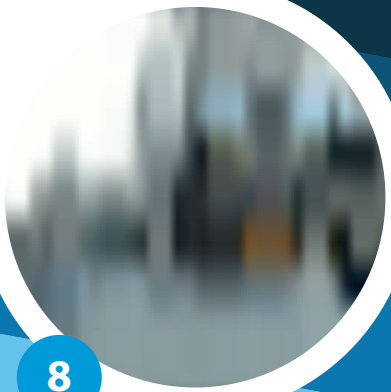
Glossary

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 another in order to decieve.

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/

National Anti-Fraud Network:
www.nafn.gov.uk
The National Anti-Fraud Network (NAFN Data and Intelligence Services) provides 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

nafn .gov.uk
Data & Intelligence Services