AASG
Accountancy AML Supervisors' Group

Payment Diversion Fraud

Extract from NECC Amber ALERT of November 2021 (Reference 0668 - NECC)

Overview

In July and August 2021, a UK retailer was the victim of a targeted, high value, payment diversion fraud (PDF) with an associated loss of c.£1.1m. This fraud contained an unusual modus operandi. This Alert provides a summary of PDF, further detail on how this specific fraud was perpetrated and what protective measures can be taken to guard against it.

PDF is the third highest harm fraud type impacting on the UK by value of reported losses. For the year to September 2021 there were 4,644 reports of PDF made to Action Fraud with reported losses of £152m.

Background

PDF involves fraudsters creating false invoices or false requests for payments, or the diversion of payments. PDF is also known as Business Email Compromise (BEC) or Mandate Fraud.

Payment Diversion Fraud

Payment diversion fraud includes the following sub threats:

- **Invoice fraud** involves a company's supplier being compromised. Typically, the victim company is contacted by the fraudsters purporting to be the supplier and requesting payment for an invoice into an account the fraudsters control.
    - There is a specific sub-category of this fraud – tradesman invoice diversion, where tradespeople are impersonated. The fraudsters identify customers and demand payments from them by impersonating the company undertaking the work.

- **Chief Executive Officer (CEO) fraud** involves fraudsters impersonating a senior executive in an organisation and contacting employees to make payments to the fraudster. The fraudsters gain access to the organisation's email accounts and gain information to enable impersonations of senior management.

- **Conveyancing fraud** targets individuals who are in the process of buying a property. Fraudsters impersonate the victim's solicitor, convincing the purchaser to redirect their payments to an account that the fraudster controls.

- **Salary diversion fraud** involves fraudsters impersonating an employee and contacting the payroll department to change the account details into which the salary is paid.

UK Retailer Fraud Incident

UK retailer was the victim of a fraud to the value of c.£1.1m. The UK retailer were engaged with a third party to assist with upgrading infrastructure. In July and August 2021, a person or persons unknown, used fictitious email addresses to trick the UK retailer's employees into believing they were corresponding with employees from the third party.

Those perpetrating the fraud also tricked employees from the third party to believe they were corresponding with employees from the UK retailer.
Fictitious e-mail addresses were used. For example:

employee@ukretalier.co.uk (retailer spelt incorrectly)
employee@thirdparti.co.uk (third party spelt incorrectly)
employee@thirdparti.fr (third party spelt incorrectly and incorrect address)

On a date in July 2021, those perpetrating the fraud used a fake retailer email address, as per the example above, and obtained from the third party details of upcoming invoice payments, their dates and invoice reference numbers. On the same date in July 2021, the UK retailer received a request purporting to be from the third party, but sent instead via those perpetrating the fraud, to send payment for upcoming invoices to a new bank account overseas. It was cited that the third party had ongoing issues with their usual bank that would not be overcome by the payment due date.

In August 2021, the UK retailer authorised the payment of £1.1m to the requested overseas bank account. Shortly afterwards, the fraud was discovered.

This fraud contained an unusual modus operandi as both the UK retailer and third party were impersonated during the fraud.

Prevent

With this iteration of PDF, when the request for payment is made it is likely to appear even more genuine due to the initial reconnaissance that has been performed, when impersonating the retailer and contacting the supplier. This will allow the fraudster to include correct details of upcoming invoice payments, dates and invoice reference numbers.

Therefore, it is important that all companies follow the protect advice set out below, regardless of how genuine a payment document may appear:

Protect your financial transactions: Before paying invoices, check the bank details are correct, especially if advised of a change in account details. The best way to check bank details is to contact the sender through known contact details, not those advising the change (e.g. existing telephone details that you have on file).

Further protect advice is available from our partners at the: National Cyber Security Centre

Report Immediately

If you think you have been a victim of PDF fraud, act quickly, contact your bank immediately as they may be able to freeze the funds before they are moved. Also, report the fraud to Action Fraud online at www.actionfraud.police.uk/reporting-fraud-and-cyber-crime or by calling 0300 123 2040.

If being either the firm, or the client, is a victim of fraud, the firm should consider whether they also suspect Money Laundering (i.e., you know there are proceeds of the crime and know where you sent the money) and therefore whether the firm should submit a Suspicious Activity Report (SAR).

Data Protection Considerations

Please consider your obligations under the relevant data protection regulations and where necessary remove any related personal data from your systems securely and within a satisfactory timeframe.

Disclaimer

The Accountancy AML Supervisors' Group (AASG) accept no responsibility for any loss, damage or expense arising in connection with the use of information in this alert. Any use will be taken to signify agreement to these conditions.

Handling advice – Legal information

This information is supplied by the UK's NCA under Section 7(4) of the Crime and Courts Act 2013. It is exempt from disclosure under the Freedom of Information Act 2000. It may be subject to exemptions under other UK legislation. Except where permitted by any accompanying handling instructions, this information must not be further disclosed without the NCA's prior consent, pursuant to schedule 7, Part 3, of the Crime and Courts Act 2013.

This report may contain 'Sensitive Material' as defined in the Attorney General's guidelines for the disclosure of 'Unused Material' to the defence. Any sensitive material contained in this report may be subject to the concept of Public Interest Immunity. No part of this report should be disclosed to the defence without prior consultation with the originator.

Requests for further disclosure which are not permitted by any handling instructions or handling code must be referred to the NCA originator from whom you received this information, save that requests for disclosure to third parties under the provisions of the Data Protection Act 2018 or the Freedom of Information Act 2000 and equivalent legislation must be referred to the NCA's Public Information Compliance Unit by e-mail on picuenquiries@nca.gov.uk"

Protecting this document

This document uses the United Kingdom's Government Security Classification System (GSCS) and has been graded as **OFFICIAL**. There are no specific requirements for storage and it can be considered safe for wide distribution within your organisation and for use in staff training or awareness programmes. However, unless otherwise specified, this information is not intended for general public dissemination and should not be included on public facing websites, external mailing lists, social media or other outlets routinely used by you to deliver information to the public without the prior and specific permission of the NCA Alerts team. We therefore request that you risk manage any onward dissemination in a considered way. This document should be disposed of by cross-cut shredder, pulping or incineration.