National Crime Agency

Amber ALERT

Payment Diversion Fraud

Date **16 November 2021**

Reference **0668-NECC**

This Amber Alert is issued by the United Kingdom's National Crime Agency (NCA). It is based on assessed intelligence and warns of dangers and threats from serious organised criminality. It is devised with the aim of bringing about preventative or remedial action.

We recommend you use this Alert to complement existing knowledge and support ongoing improvements to your business processes and procedures.

The threat of payment diversion fraud within the retail industry.

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.

What We Would Like You to Do

This Alert is being shared under Section 7 of the Crime and Courts Act 2013 for the prevention and detection of crime. Please note the handling conditions provided on page 6 of this Alert.

The retail sector may use this information to inform their approach to identifying and mitigating the threat associated with PDF.

The National Crime Agency (NCA) is a national law enforcement agency which leads the UK's fight to cut serious and organised crime. The NCA Alerts process is the way in which we provide information to non-law enforcement bodies including the private sector to combat and disrupt serious crime. To help us to improve this service, we would welcome any feedback you have on both the Alert itself and the information provided to you. Please email all feedback to alerts@nca.gov.uk and include **Reference 0668-NECC** in the subject line.

Payment Diversion Fraud

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 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

A 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.

Data Protection Act

The NCA reminds you of your legal obligations in respect of the management of this information, including under the Data Protection Act 2018

Article 5(1) requires that personal data shall be:

1. Processed lawfully, fairly and in a transparent manner;
2. Collected for a specified, explicit and legitimate purpose and not further processed in a manner that's incompatible with these purposes;
3. Adequate, relevant and limited to what's necessary in relation to the purpose for which they are processed;
4. Accurate and where necessary kept up to date;
5. Kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed;
6. Processed in a manner that ensures appropriate security of the personal data.

Disclaimer

While every effort is made to ensure the accuracy of any information or other material contained in or associated with this document, it is provided on the basis that the NCA and its staff, either individually or collectively, accept no responsibility for any loss, damage, cost or expense of whatever kind arising directly or indirectly from or in connection with the use by any person, whomsoever, of any such information or material.

Any use by you or by any third party of information or other material contained in or associated with this document signifies agreement by you or them to these conditions.

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.

Alert Markings

NCA Alerts are marked either Red or Amber. This is designed to indicate the urgency of the warning. Red may indicate a more immediate or specific threat, whilst those marked Amber will provide more general information that may complement existing knowledge.

NCA Alerts Team

Recognising that the private sector is often the victim of serious organised crime and is engaged in its own efforts to prevent, deter and frustrate criminal activity, the NCA seeks to forge new relationships with business and commerce that will be to our mutual benefit – and to the criminals' cost. By issuing Alerts that warn of criminal dangers and threats, NCA seeks to arm the private sector with information and advice it can use to protect itself and the public. For further information about this NCA Alert, please contact the NCA Alerts team by email alerts@nca.gov.uk. For more information about the National Crime Agency go to www.nationalcrimeagency.gov.uk.

Protecting the Public – Providing information back to the NCA

Section 7(1) of the Crime and Courts Act 2013 allows you to disclose information to the NCA, provided the disclosure is made for the purposes of discharging the NCA's functions of combating serious, organised and other kinds of crime. The disclosure of such information to the NCA will not breach any obligation of confidence you may owe to a third party or any other restrictions (however imposed) on the disclosure of this information. The disclosure of personal information about a living individual by you to the NCA must still comply with the provisions of the Data Protection Act 2018 (DPA). However, you may be satisfied that the disclosure by you of such personal information to the NCA in order to assist the NCA in carrying out its functions may be permitted by Schedule 2, Part 1 of the DPA 2018. This allows a data controller to be exempt (by means of a restriction or adaption) from provisions of the GDPR, if the personal data is processed for the following purposes:

a) the prevention or detection of crime,
b) the apprehension or prosecution of offenders, or
c) the assessment or collection of a tax or duty or an imposition of a similar nature,

to the extent that the application of those provisions of the GDPR would be likely to prejudice any of the matters mentioned in paragraphs (a) to (c).
(DPA 2018, Schedule 2, Part 1).

Any Section 7(1) information should be submitted to alerts@nca.gov.uk.

The NCA's Information Charter is published on our external website at www.nca.gov.uk

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 Statutory Disclosure Team by e-mail on statutorydisclosureteam@nca.gov.uk.