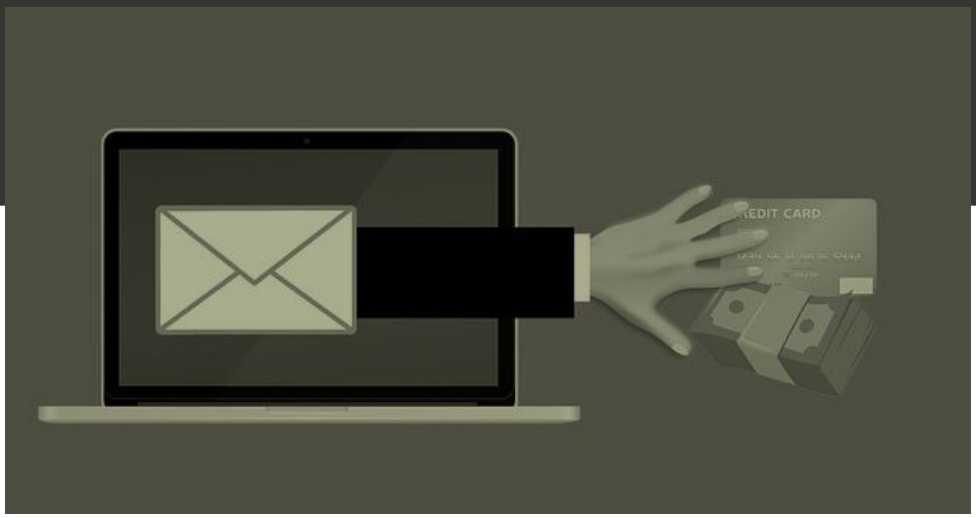
FPLG
FOR PURPOSE LAW GROUP
A Professional Law Corporation

GENERAL

Payment Diversion Fraud in the Charitable Sector

02.26.24 | Linda J. Rosenthal, JD



"Making sure that you are paying the correct party is key."

That's the deceptively simple – but urgent – advice to charitable entities, large and small, from a leading anti-fraud expert at BDO UK, a cosponsor of Charity Fraud Awareness Week 2023 and contributor to *Charity Fraud Report 2023.*

"Payment diversion fraud" (PDF) has been one of the major threats in recent years in the charitable sector, causing enormous financial and non-financial losses, explains Kaley Crossthwaite, CA, Head of Quality and Risk Management at BDO UK. It "happens when a fraudster impersonates a supplier by creating or amending what appear to be genuine invoices or other payment requests to divert funds to bank accounts under their control." The scheme "… largely relies" on wrongdoers being able to pose as someone they are not…." in order to elicit payments from an unsuspecting organization.

In many cases, adds Ms. Crossthwaite, "[t]here is an entire industry underpinning this type of fraud," and "going to great lengths to ensure that fraudulent requests look genuine."

What is It?

For convenience in this post, we're using the most familiar and straightforward label for this category of fraud: namely, "payment diversion fraud" (PDF). However, several other terms regularly pop up in the literature.

Garden-variety PDF is where "fraudsters interfere with the payment process of legitimate charities and divert payment to their own account." It's a wrongful practice by bad actors "creating false invoices or false requests for payments, or the diversion of payments."

Alternate terms are often used interchangeably with PDF although the substitute labels more correctly apply in subtly different situations. The most notable are: "Authorised Push Payment Fraud" [pretending to be a bank representative]; "Bank Mandate Fraud" [fooling charity into changing the direct deposit details of legitimate payees, substituting the banking information of the bad actors].

Others examples are: Business Email Compromise (BEC); Invoice Fraud; Chief Executive Fraud (CEO); and Salary Diversion Fraud.

Common Examples

However described, it's "certainly on the increase. Fraudsters use sophisticated spear-phishing techniques such as impersonating a key supplier or an organisation's bank to trick employees into changing bank details or making payments." See *Payment Diversion Fraud – What is it? and how to protect your business from it* (December 8, 2021) Chris George, Head of IT, CEME Ltd, *linkedin.com/pulse;linkedin.com/pulse.*

The first contact – perhaps a phone call – from a "fraudster phishing for information" is "often portrayed as an 'urgent' request," according to Mr. George. "Even seemingly harmless responses could aid a more targeted attack, such as the impersonation of a trusted colleague or the mimicking an invoice from a key supplier."

Similarly, the anti-fraud experts with the UK's National Health Service describe a typical scenario of payment diversion fraud: "fraudsters creating false invoices or false request for payment, or the diversion of payments in order to defraud you or your organisation… See *Payment Diversion Fraud*, Counter Fraud Authority, *cfa.nhs.uk.*

The wrongdoers' focus starts with the staff of a charity's finance or procurement department. "An email which appears to come from a known supplier is sent by the cyber-criminal to a member of staff. The email will request that future payments for products or services are made to a new bank account and will give a reason for the account change. The new account will be under the control of the cybercriminal and any funds paid into it will be lost."

At Preventing Charity Fraud, the website of the organizers of Charity Fraud Awareness Week, experts offer helpful information and guides. See, for example: *Invoice fraud*, a "Tackling Charity Fraud Case Study." There, a hypothetical charity supporting cancer patients is defrauded of large amounts of money resulting from a "bogus change to a supplier's bank account details."

The authors continue: Following a common pattern, the charity "received an email purportedly from a regular supplier asking for their bank account details to be changed." The request was forwarded to the finance department which processed two payments to the supposed new account. The legitimate supplier, after two missed payments, contacted the charity.

"Internal enquiries established" that the rather sloppy fake letter – undated, with poor grammar, and showing a sort code and account number not matching the legitimate business's bank branch – slipped through the system easily.

More Creative Scams

Chris George, the Head of IT at CEME Ltd (quoted earlier), confirmed that the "most common approaches" made by fraudsters" resemble these same scenarios: that is, in "a phone call or via email, the impersonator '… will claim to represent a known supplier.'"

But his UK firm has also "investigated some very elaborate scams" that were successful at least until they were discovered: For instance:

- An imposter purporting to be the CEO asks an employee to move funds urgently to a secure location amidst a supposed cyber attack
- Fraudsters pretend to be from the charity's bank. They call, warning of a failed payment, convincing an employee to "provide sufficient information to allow [them] to log onto the organisation's bank account to set-up new payments."
- Criminals pose as to be suppliers, called charity employees repeatedly to pressure them to change payment details and immediately pay one or more invoices. Various reasons are given, including the lie that the supplier "may go out of business" soon.

For excellent information about payment diversion fraud and its diabolical variations, check out:

- *What is payment diversion fraud, and how can you avoid it?* (January 4, 2022) Tim Mitchell, Content Director, Get Safe Online, *preventcharityfraud.uk.org*
- *Payment Diversion Fraud – What is it? and how to protect your business from it* (December 8, 2021) Chris George, CEME Ltd, *linkedin.com/pulse*
- *Payment Diversion Fraud*, Counter Fraud Authority, *cfa.nhs.uk*
- *What is Payment Diversion Fraud?* (March 14, 2022) James Hyland & Co., *jhyland.com*
- *Payment Diversion Fraud: What Does It Look Like* (May 15, 2022) James Hyland & Co., *jhyland.com*
- *Charities: Don't just take steps to prevent fraud – be aware and prepare* (November 9, 2022) Jamie De Souza, Esq., & Emily Sharples, Esq., Trowers & Hamlins LLP, *preventcharityfraud.org.uk.*
- *Charity fraud examples you should watch out for in 2023* (April 14, 2023) Jenny Phipps, *qlicnfp.com*
- *Outward Bound – Fraud in the Procurement Cycle* (May 18, 2023) Kaley Crossthwaite, CA, Partner, Head of Quality and Risk Management, *bdo.com.uk*
- *Payment diversion fraud poses significant threat to businesses* (September 7, 2023) *hiscoxgroup.com*

See also, of course, the latest *Charity Fraud Report 2023* as well as the ones from 2022 and 2021 by Charity Fraud Awareness Week cosponsors BDO UK and the Fraud Advisory Panel.

How Are These Scams So Successful?

According to Alana Muir, Head of Cyber at Hiscox UK: "Payment diversion fraud is the gift that keeps on giving for cyber criminals and can pose a significant threat to any [entity]. Most attacks happen because [the target organizations] fail to carry out basic checks before making a payment – it's human error and often avoidable…."

"The first question to ask," according to CEME Ltd's Chris George, is ''Why do we fall for payment diversion fraud?'"

He adds: Even in the "extreme examples" that he describes, the situation to those at the charity "appeared real….: " Continuing, he explains: "Well the first thing to think about is, how many times do you respond to a request without thinking twice? Payment diversion fraud is effective because it feeds on our trust and sense of obligation, whether at work or in our personal life."

On a more optimistic note, Mr. George offers "some red flags to look out for when deciding whether an email is genuine or not…" For example, first "be mindful of email addresses. Fraudsters often use email addresses that are similar but not the same as the addresses you trust…."

In addition, consider the nature of any requests. "Are you being asked to do something outside the normal scope of your role? Would you expect this to be asked of you? If the answer is no, then this should raise suspicions, especially if the request comes with a sense of urgency or time pressure."

In connection with any money transfers: "Are you being asked to transfer money in a way that doesn't follow … normal processes? That could indicate fraud."

And are there any "requests to restrict communication?" "Being asked to confine communications to email, or being asked to keep the transaction confidential," may indicate the request is not genuine.

"Context" can "play a very important role in stopping payment diversion fraud," Chris George elaborates. "Criminals are developing increasingly sophisticated techniques, where they can replicate or even have access to a trusted colleague's email. In these circumstances, the knowledge that we have of one another plays an important part in detecting when something is wrong. If the tone, language or the request itself seem out of character in an email or message from a colleague – and especially so if from a senior figure – always act on it and flag your suspicions to the right person."

Prevention and Mitigation of Loss

It's critical for all charities of any size to perform periodic risk-management reviews and to put into place adequate controls for both prevention as well as mitigation of loss in the event a fraudster is successful.

See, for example, the "top tips" for prevention in the final section of the *Charity Fraud Report 2023*. Under the topic "Payment Diversion Fraud," there are several suggested steps:

- "Introduce a robust internal policy for changing supplier account details or making one-off payments to new bank accounts
- Only change payment details if you have verified the details directly with the supplier on a phone number that is already known to you and following consultation with your reporting manager
- Educate employees so they understand the many guises that payment diversion fraud may take

- Implement a built-in phishing email identifier into your charity's email system to flag unusual or suspicious emails upon receipt."

"Regardless of how genuine a payment document may appear," these experts advise, "there is no such thing as being too cautious."

Most of the articles cited above include invaluable tips on prevention. See, particularly, the extended discussion of "payment diversion fraud" in *Outward Bound – Fraud in the Procurement Cycle* (May 18, 2023) Kaley Crossthwaite, CA, Partner, Head of Quality and Risk Management, *bdo.com.uk*.

Conclusion

This post rounds out our first group of deeper dives on the important topic of charity fraud, following up on our four-part series reporting on Charity Fraud Awareness Week 2023. See *Procurement Fraud in the Charitable Sector* (February 11, 2024) and *Expenses Fraud in the Charitable Sector* (February 19, 2024).

These three dangers have been vying for the past three years for the second and third spots of "most reported fraud incidents." See the *Charity Fraud Report 2023* as well as the ones for *2022* and *2021*.

The top spot during that entire period has been held by "Misappropriation of Cash or Assets." There is little to indicate that this troubling – and broad – category of charity fraud will be knocked off that perch anytime soon. We'll save that tantalizing topic for a bit later, after we cover a few additional danger categories.

– Linda J. Rosenthal, J.D., FPLg Information & Research Director