# Fraud Alert

tiaa

## Mandate Fraud Using Creative Education Details

A Mental Health NHS Foundation Trust has been targeted by fraudsters with an attempted mandate fraud.

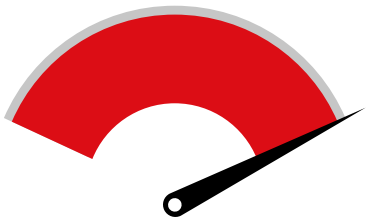
A Clinical Lead at the Trust received an email purportedly from the Project Manager of Creative Education chasing up an invoice payment and subsequently requesting a change of payment details.

The email contact from Creative Education initially appeared to be genuine as it came from xxx@creativeedvcation.com. The fraudsters had further attempted to deceive the Trust by using the correct contact details of the Project Manager. The correct email account should be xxx@creativeeducation.co.uk.

Considering the detail that the fraudsters had used in the email address and the use of the correct details for the Project Manager, it would appear that the email accounts had been hacked.

**Note the u was changed to a v and .co.uk was changed to .com**

**These fraudulent email addresses often contain a small change in detail that is difficult to spot.**



**Status: Action Required**

**Check if your organisation makes any payments to Creative Education and be alert to correspondence requesting a change of bank details.**

**If you think that your organisation has been a victim of mandate fraud, please notify your bank immediately to attempt to recover lost funds, and alert your Anti-Crime Specialist.**

## How to protect your organisation from fraud

Before changing any supplier bank account details (direct debit, standing order or bank transfer mandate), **always** contact the supplier using established contact details in existing records and not from information supplied in a change request.



For further discussion and support, including fraud awareness training services, contact:

**Melanie Alflatt, Director of Anti-Crime Services** ■ Email: **fraud@tiaa.co.uk**

**www.tiaa.co.uk**

**0845 300 3333**