Hampshire and Isle of Wight Fraud and Security Management Service
Hosted by North Hampshire Clinical Commissioning Group

LOCAL FRAUD PREVENTION NOTICE 01 2016-2017

To:	Practice Managers, Finance Managers
CC:	Risk Managers, Communications Managers
Subject:	CEO Fraud – Local Incidents
Author:	Alec Gaines, Local Counter Fraud Specialist
Date:	21/11/2016

BACKGROUND

We are continuing to see a steep rise in the number of reports of 'CEO' fraud. CEO fraud isn't fraud committed by a Chief Executive Officer, but instead is the generic term given to a fraud where the fraudster impersonates a Director or similar from an organisation and requests an urgent transfer of funds. These frauds can be very professional, and are often committed by organised fraud gangs based outside of the UK.

The fraud works by the fraudster sending an email to a Director of Finance, Chief Finance Officer, Practice Manager or member of a Finance team. It will purport to be from the organisation's Chief Executive Officer, or another high ranking executive, such as the Chair of the organisation. The content of the email can be similar to: "can't talk now, in a meeting but need an urgent transfer of funds". Bank details for a money transfer are then provided. Any funds transferred are quickly laundered and in all likelihood will already be in an overseas account before the fraud is even identified.

At first glance some requests can appear genuine; it isn't difficult to adjust the appearance of an email in MS Outlook so it appears that it has come from a different email address than the reality. In some cases the fraudster has registered an external email account in the name of the person he is impersonating.

A number of such attempts have been reported within Hampshire in the past year. Across the country £32 million has been reported as lost as a result of this type of fraud, with one private healthcare company losing £18.5 million. This weekend a GP Practice in Hampshire was successfully targeted and lost £18k and in the last week the CFO of a Hampshire Hospital Trust was unsuccessfully targeted.

ACTION

Employees should be alerted regarding this type of fraud and organisations should have a system in place which requires staff to properly verify contact from their CEO or senior members of staff before taking action on any such requests; for example having two points of contact so that the staff can check that any instruction they have received is legitimate.

TIMESCALES

This action should be undertaken with immediate effect if not already in place.