

## Internal TSA Briefing Note May 2011

### Recent fraudulent activity targeted at the RP sector

#### Introduction

The TSA has received information in recent weeks about a significant number of actual and attempted frauds targeted at registered providers (RPs) and their suppliers. These involve diverting legitimate supplier payments from RPs into bank accounts controlled by the fraudsters. We understand that similar fraudulent activity was targeted at local authorities and building companies over the last year.

#### The fraud

The fraud is facilitated by RPs acting upon what appear to be legitimate requests to implement changes to suppliers' bank account details. We understand that letters used to generate changes are credible because they replicate companies' headed paper, contain relevant details about the companies and appear to have genuine and original signatures of authorised personnel. They are often supplemented by friendly, 'helpful' telephone contact from persons knowledgeable about the companies. A number of development and maintenance suppliers have been targeted across the country. Those we are aware of and which involve RPs are as follows [*summary only*]:

Name / Location	Date	Amount	Type
London	June 2010	nil	Attempt to change bank details
London	Oct 2010	nil	Attempt to change bank details
London	Feb 2011	nil	Attempt to change bank details
North West	Mar 2011	£240k part recovered	Bank details changed
Merseyside	Mar 2011	£1.1m recovered	Bank details changed
North West	Mar 2011	£100k	Bank details changed
London	April 2011	£807k recovered	Bank details changed
Kent	April 2011	£230k	Bank details changed
Hampshire	April 2011	£813k recovered	Bank details changed
	May 2011	£165k at risk	

It can be seen from the table that the activity is spread across the country. It is notable that, despite the sophistication of the fraudulent documentation, the fraudsters have not managed to access most of the funds before either the RPs or the banks took action to prevent monies being moved on. It is difficult to assess why this is the case because the banks do not generally share such information with their clients.

### **Regulatory response**

Where RPs bring individual cases to our attention we should follow up their responses as appropriate and in line with the regulatory framework.

Where regulatory staff have planned or ad hoc engagements with RPs they should draw their attention to this recent systematic fraudulent activity and remind them that they should have a clear and well-communicated fraud policy and response plan covering prevention, detection and reporting of fraud, the recovery of assets, and action to be taken against perpetrators. It would also be appropriate to advise RPs that they should review their internal controls over changes to bank details and consider implementing additional checks to verify information received from suppliers.

### **Registered Provider responses**

RPs should follow their fraud policy which may include reporting the matter to their local police force. The City of London Police has a website which summarises fraud reporting and sources of information:

[www.cityoflondon.police.uk/CityPolice/Departments/ECD/Fraud/reportfraud.htm](http://www.cityoflondon.police.uk/CityPolice/Departments/ECD/Fraud/reportfraud.htm)

They also oversee the National Fraud Intelligence Bureau which is collating data on frauds. Information should be passed to the NFIB by local police.