



# Online Marketplace Fraudster: Targeting Jobseekers

October 2017

Copyright © City of London Police 2017

CoLP Disclaimer: While every effort is made to ensure the accuracy of the information or material contained in this document, it is provided in good faith on the basis that the Commissioner, the City of London Police and its police officers and staff accept no responsibility for the veracity or accuracy of the information or material provided and accept no liability 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 information or material herein. The quality of the information and material contained in this document is only as good as the information and materials supplied to the City of London Police. Should you or your police force hold information, which corroborates, enhances or matches or contradicts or casts doubt upon any content published in this report, please contact the City of London Police by return.

Any use of the information or other material contained in this document by you signifies agreement by you to these conditions.



To help prevent your business to counter fraud and/or to obtain details of our available courses, please contact the City of London Police Economic Crime Academy via our website <http://academy.cityoflondon.police.uk> or you can view our latest prospectus on <http://academy.cityoflondon.police.uk/images/prospectus>

## How do Online Marketplace Fraudsters Operate and how are they targeting Jobseekers?

Fraudsters typically offer bogus goods for sale online via an online marketplace account set up with fraudulent details. Once a victim has committed to purchasing the goods from the fake account, the fraudster sends a bogus email purporting to be from an established escrow\* provider. After convincing the victim to transfer their money to the escrow for safekeeping, the fraudsters sever all contact and either delete or abandon the fraudulent account.

Action Fraud has received intelligence suggesting that rather than setting up fraudulent accounts, fraudsters are advertising bogus online sales roles on job vacancy websites in the hope of attracting unsuspecting jobseekers. Once a jobseeker has shown interest, the fraudsters tell them they will be selling goods on the company's behalf; often the goods are cars or machinery but they could be anything. Jobseekers are also instructed that they must use their own personal pre-existing bank accounts and payment methods, as well as their own online marketplace accounts. The fraudsters usually give a vague excuse as to why a business account or login is not available. Jobseekers are then sent photos and information of the products they will be selling (which do not exist) in order to create an attractive advert to entice the primary victim; the buyer of the goods. Once the victim has transferred their money to a bogus escrow provider, no goods are ever received and all contact is severed. This leads to a financial loss for the buyer of the goods as nothing is ever received. Likewise, the recruited jobseeker receives none of the promised payment for their work as originally stipulated in the bogus advert.

\*Escrow – An escrow is a type of agreement where a third party becomes involved in a financial transaction; an escrow provider will hold a sum whilst the transfer of goods or services is facilitated between two other parties. Upon transfer, the escrow provider will then release the funds as appropriate. Genuine escrow providers can be useful, however fraudsters frequently impersonate them for their own financial gain.

## Protect Yourself

### Buyers

- When making a large purchase such as a new car or machinery, always meet the seller face to face first and ask to see the goods before transferring any money.
- False adverts often offer goods for sale well below market value to entice potential victims; always be cautious.
- Exercise caution when sellers state that they are selling on behalf of a friend, colleague or business.

### Jobseekers

- Don't assume advertised vacancies have been verified by the website or classified advertisement sites upon which they feature. If you suspect a job vacancy to be fraudulent, be sure to notify the website via their reporting/flag functions. Doing so prevents others from becoming victims of fraud and helps organisations and law enforcement tackle and disrupt fraudulent activity.
- Although many legitimate job vacancies are internet based sales roles, those which are vague about the business, product type, sales method or sales platform to be used should be approached with caution. It is always good practice to conduct further enquiries about an advertised role.
- Genuine businesses would never ask you to use your personal bank or online payment accounts to facilitate business transactions, nor would they ask to utilise your personal online marketplace account in order to sell their products. If someone claiming to represent the organisation suggests you do this or asks for your personal details so they can use your account(s) themselves, sever contact.

## Handling Instructions

---

This report may be circulated in accordance with the protective security marking shown below and caveats included within the report. The information contained in this report is supplied by the City of London Police in confidence and may not be shared other than with the agreed readership/handling code without prior reference to the City of London Police. Onward disclosure without prior authority may be unlawful, for example, under the Data Protection Act 1998.

The cover sheets must not be detached from the report to which they refer.

<b>Protected:</b>	<b>NOT PROTECTIVELY MARKED</b>
<b>Suitable for Publication Scheme:</b>	NO
<b>Version:</b>	V1.0
<b>Storage File Location:</b>	G:\OPERATIONAL\FRAUD DESK\Action Fraud Crimes\21. Volume Crime Team\Researcher\Alerts\2017
<b>Purpose:</b>	Fraud Alert
<b>Owner:</b>	NFIB Management
<b>Author:</b>	104068p
<b>Review By:</b>	Team Supervisor