National Fraud Intelligence Bureau

CITY OF LONDON POLICE
National Policing Lead For Fraud

Monthly Fraud Threat Update

August 2017

Copyright © City of London Police 2017

NFIB Disclaimer: While every effort is made to ensure the accuracy of the information or material contained in this Alert, 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 Alert, please contact the City of London Police NFIB by return.

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

CITY OF LONDON POLICE
Economic Crime Academy

To help you to prevent fraud and/or 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

Key Judgements:

Impact on Individuals:

- Job Application Ransomware
- Horse Racing

Impact on Enterprise:

- GP Practices being targeted for CEO Fraud

Cross Cutting Themes:

N/A

Introduction

This monthly threat update will provide an overview of the trends affecting individuals and enterprise as reported to Action Fraud. This report incorporates an assessment of information received during the period of 1st July – 31st July 2017. We welcome your feedback so that we can shape future reports to your needs.

Banking and Corporate

GP Practices being targeted for CEO Fraud

GP practices in the UK have received contact from suspect(s) purporting to be their director / practice manager who have asked for funds to be transferred into several UK bank accounts. The suspects were successful in two of the reports.

Cyber

Job Application Ransomware

July saw the return of the fake job application ransomware campaign. This campaign involves suspects sending out large quantities of phishing emails pretending to be looking for a job within the victim's company. This appears to come from a random email address and the subject header reads 'Job Application'.

From analysis of the contained attachment (the CV) header, if opened it executes a file which is currently thought to contain a type of ransomware.

Investment Fraud

New Commodity: Horse Racing

The Investment Fraud team have identified a new commodity in investment fraud which involves investments in horse racing. Currently there are two companies offering this investment which the team are aware of. The companies claim to specialise in horse race betting using computer analytic software and that the software does all the work so that the victim does not need to. Victims are known to be contacted by post / brochures / leaflets.

Volume

Modelling Platform

Victims have reported being approached with bogus offers of modelling work through a modelling platform which matches models and photographers. Victims are paid in advance with cheques or travellers cheques for a greater value than agreed, but then instructed to pay the "additional" money onto makeup artists and stylists. The victims transfer the "additional" money from their own expenses to three bank accounts, prior to discovering that the original cheques were false. The cheques have then subsequently bounced, leaving the victims out of pocket.

Glossary of Terms

Ransomware	This is a form of malware that attacks your computer, locking you out and demanding payment in the form of a 'fine' or 'ransom' to have it unlocked.
Phishing	Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by illegally impersonating a trustworthy entity via an email.

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.

Protective Marking:	**NOT PROTECTIVELY MARKED**
FOIA Exemption:	NO
Suitable for Publication Scheme:	NO
Version:	FINAL
Storage File Location:	
Purpose:	Provide an overview of key themes affecting individuals and enterprise. The information contained within this report has been based upon content within Action Fraud reports which have not been verified as true and accurate accounts.
Owner:	NFIB
Author:	Senior Analyst, 74545n
Review By:	Senior Analyst, 105433