

R v Daniel Levi & Others (2005)

Preston Crown Court 1 November 2005

Court finds gang guilty of conspiring to defraud following phishing scam involving eBay customers.

The Case

The accused, his brother, an accomplice and several money laundering mules were involved in a scam which involved the online harvesting of thousands of email addresses every hour through the use of an email address collection programme.

The attackers then made use of Windows Desktop 2000 software to make it appear that emails sent by them originated from an eBay server under the email address "aw-confirm@ebay.co.uk". The email contained eBay branding and lead customers of the online bidding site to believe that eBay was updating their records and that a link to the update page should be followed in order to proceed with the process.

The web link contained in the email took consumers to a web page hosted on the computer of an accomplice, Mr Daniel Lett and prompted persons to divulge usernames, passwords and sometimes banking account details. Around 2,000 people unwittingly divulged their confidential information.

The gang then utilized the usernames and passwords divulged to them to hijack current eBay retailer accounts, lock the true owners out by changing their passwords and then, using the retailer's good record, offered items such as watches and laptop computers at incredibly low prices to bona fide eBay customers.

Buyers who showed interest in the items were sent an email offering even further discounts on the items if they made use of CHAPS, same day payment transfers, instead of eBay's proprietary payment service. Buyers dispatched payments to the mules' accounts and were never sent the items they had bought. Over 160 customers were duped in this way between July 2003 and

July 2004.

The multiple fraudulent acts by the gang resulted in close to £200,000 being stolen from unsuspecting members of the public, although police estimates were pitched at around the £500,000 mark.¹ Property seized from the gang included two BMW motor vehicles and thousands of pounds worth of computer equipment.

Decision

The Crown Court found Mr Daniel Levi guilty of conspiracy to defraud, conspiracy to launder money and perverting the course of justice. The court sentenced Mr Levi to four years imprisonment for his actions.

His brother, Guy Levi, received twenty one months for his part in the conspiracy to defraud. The accomplice and computer expert, Mr Daniel Lett was sentenced to two years imprisonment for conspiracy to defraud.

A number of money laundering mules including Derek Anderson, 59, Chris Worden, 23, Craig Jameson, 31 and Gareth Rice, 22, were also sentenced to six months in prison for their money laundering activities. It was held that the mules should have been aware or should reasonably have suspected that the monies given to them had originated from the proceeds of crime. A number of other mules escaped prosecution due to lack of evidence.

Commentary

The Levi gang was charged in terms of the common law crime of conspiracy to defraud and the Proceeds of Crime Act 2002 (POCA).

A conspiracy is defined in terms of the Criminal Law Act 1977 under section 1(1) and section 1(2), as follows: "... if a person agrees with any other person or

persons that a course of conduct should be pursued which, if the agreement is carried out in accordance with their intentions, either;

- will necessarily amount to or involve the commission of any offence or offences by one or more of the parties to the agreement, or
- would do so but for the existence of facts which render the commission of the offence or any of the offences impossible, he is guilty of conspiracy to commit the offence or offences in question."

This conspiracy must also be coupled with an intention to commit a particular, formally defined crime as was defined in the judgment of Buckley J, in *In Re London and Globe Finance Corporation Limited*² where it was stated that in order to be found guilty of conspiracy to defraud the "fraud" element is satisfied by the use of "deceit to induce a (particular) course of action".³ This was obviously evident from the conduct of the digital fraudsters.

The definition of this crime is wide enough to indict numerous online fraudsters in a variety of well formulated ways which could be extended to include other online fraudulent activity such as pharming.

In terms of the POCA a number of offences are created under Part 7, more particularly sections 340, 327, 328 and 329, some of which were the basis of indictment against the Levi gang and should be more widely used in the sphere of internet based fraud.

- Section 340 (3), clearly defines the concept of what criminal property arising from criminal activity is: "... property is criminal property if; (a) it constitutes a benefit from criminal conduct or it represents such a benefit (in whole, or part and whether directly or indirectly), and (b) the alleged offender knows or suspects that it

constitutes or represents such benefit.”

● Section 327, creates offences regarding the concealing, disguising, converting, transferring or removing of criminal property from the UK.

● Section 328, dictates that it is an offence to enter into becoming concerned in an arrangement whereby the party “knows or suspects facilitates (by whatever means) the acquisition, retention, use or control of criminal property, by or on behalf of another person.”

Mr Levi and his gang of fraudsters are, contrary to recent newspaper reports, not the first persons to be sentenced in the UK for phishing related fraud scams. In June 2005, two other men Douglas Harvard and Lee Elwood were sentenced to six years and four years respectively for conspiracy to defraud and conspiracy to launder money resulting from their phishing activities, which activities netted them in excess of £6.5million in a two year period. The only real difference between the two cases is that the Levi gang was harvesting its own information, whereas the Harvard and Elwood pairing were making use of stolen information supplied to them by Russian accomplices.

Although the case of the Levi gang may mark a milestone as far as bringing these particular fraudsters to book, the case highlights the fact that the traditional fraudster is using the constant advances in technology as a way of finding new methods to defraud unsuspecting victims. Whilst the conviction of the Levi gang is to be welcomed, it also shows the constant battle the police face in securing convictions in an ever changing technological war where the fraudster simply migrates to a new area of fraud as soon as the area he was previously operating in is closed.

This is certainly best illustrated by the advent of new chip and pin based credit cards, which has dramatically changed the modus operandi of the traditional, “steal the card and use it” fraudster. These criminals can now operate on a scale of which the traditional credit card fraudster can only dream.

In the Netherlands for example, a recent police raid dismantled a network of over 100,000 linked computers which had been infiltrated globally by only three Dutch nationals. The computers were used to phish for online usernames and passwords as well as to extort money from corporations by threatening to overload their servers with diverted internet traffic.⁴

Other reports have suggested that top young computer brains are being poached by online fraud gangs, luring them with large cash incentives by way of online chat rooms, to work as full time phishing experts. These “coders” are often as young as sixteen and make more money from their frauds than most adults see in a lifetime.

Recent figures released by the Association of Payment and Clearing Services has shown that card not present fraud has increased for the first half of this year to £90.6million, up twenty nine per cent for the same period in 2004. Online fraud has also accounted for more than twenty five percent of all fraud losses during that period.

What is worrying about those statistics is that in contrast to the £90million lost to these fraudsters since January 2005 and the extended powers granted to the police in terms of the statutory sections mentioned above, the reported cases indicate that the High Tech Crime Unit has only secured two convictions this year,

one of which was a result of direct phishing activity.

A recent US House Committee on Financial Services has indicated that 10 million Americans were affected by phishing based identity theft last year. Those victims spend around 90 hours and \$1,700 each correcting the problem.⁵

Conclusion

The Preston Crown Court should be praised for the decision in this case as it shows that there is an effective deterrent for those who are caught. However, the cost of phishing scams cannot be ignored and the occasional successful conviction will not deter most fraudsters who do not believe they will be caught.

The migration of fraud from traditional methods to the digital age must be constantly reviewed and more effective remedies be found, whether this be by way of better security to make the cost of trying to commit the crime prohibitive or the seizure of the fraudster’s assets so that it is clear that crime does not pay. It is only then that the public may be kept safe from gangs such as Mr Levi’s.

Anthony Riem Partner
Philippsohn Crawfords Berwald Solicitors
ajr@pcblitigation.com

1. www.out-law.com, 2 November 2005
2. [1903] 1 Ch 728 at 732
3. Smith and Hogan - Criminal Law (11th Edition 2005)
4. www.newscientist.com, 12 October 2005
5. Reuters, 10 November 2005