Crime and gambling: A brief overview of gambling fraud on the Internet

Mark Griffiths[1]

ABSTRACT

Although there is an association between crime and gambling there is relatively little information and research on the topic. One area that appears to have become more prevalent over the last five years is that of fraudulent gambling activities on the Internet. This paper briefly outlines how many frauds and scams have moved into technological media such as the Internet and overviews a number of these including: (i) lottery scams, (ii) fake gambling site scams, (iii) betting software scams, (iv) gambling 'bonus' scams, (v) 'twofer' scams, and (vi) prize scams. It is concluded that gambling fraud on the Internet is a growth area because many gamblers themselves want to get a huge reward from a small outlay (just as the fraudsters do). As long as there are people who are prepared to risk money on chance events, there will be those out there who will want to fraudulently take their money from them. Given the complete lack of empirical data on these fraudulent practices, there is a need for research to be initiated in this newly emerging area of criminological concern.

Crime and gambling: A brief overview of gambling fraud on the Internet

Although there is an association between crime and gambling there is relatively little information and research on the topic. According to Smith, Wynne and Hartnagel, (2003), gambling related crime tends to relate to one of four distinct types. These are:

- *Illegal gambling* – Gambling activity that is counter to jurisdictional regulations statutes, such as operating without a gambling license, cheating at play, etc. Other authors have examined illegal ways that players get money from particular forms of gambling such as slot machines (see Griffiths [1994] for an overview of illegal ploys used to make money from slot machines in the UK).
- *Criminogenic problem gambling* – Activities such as forgery, embezzlement, and fraud, typically committed by problem gamblers to support a gambling addiction (Yeoman and Griffiths, 1996; Griffiths and Sparrow, 1998).
- *Gambling venue crime* – Crimes that occur in and around gambling locations, such as loan sharking, money laundering, passing counterfeit currency, theft, assault, prostitution and vandalism. There is also other specific gambling-related criminal activity involving violence against gaming industry employees usually as a result of when gamblers lose money in betting shops (Griffiths and Hopkins,

[1] Dr. Mark Griffiths (BSc, PhD, PGDipHE, CPsychol) is professor of gambling studies and Director of the International Gaming Research Unit at Nottingham Trent University.

2001) or amusement arcades (Parke and Griffiths, 2004; Griffiths, Parke and Parke, 2005).

- *Family abuse* – Victimization of family members caused by another family member's gambling involvement, (e.g., domestic violence, child neglect, suicide, and home invasion) (Griffiths, 2006).

However, one form of gambling related crime that is not specifically covered in Smith et al's list is that of fraudulent gambling activities on the Internet (Griffiths, 2000). This may be in part due to the fact that the authors have not kept up with technological advances and/or may not have been aware of such types of new criminal activity. Therefore, this short paper briefly overviews the main types of gambling fraud on the Internet.

Hi-tech fraudulent gambling scams

When it comes to fraud, gambling scams are a profitable area because fraudsters play on the psychology of human greed. At a basic level, some of the most common types of gambling fraud simply involve online gambling sites taking a gambler's money without paying out winnings (Griffiths, 2003a). Some online fraudsters construct systems that are impossible to win at. The probabilities of winning are miniscule, and when the gambler decides to stop playing, the remaining money deposited into the online gambling account becomes inaccessible. Other small-scale fraudulent activities include claims by an online gambling site that it is Government licensed or has been given a 'kitemark' of 'good social responsibility' (i.e., some kind of third party accreditation) by a reputable organisation. These are used to gain the gambler's trust which in turn may lead to them gambling on their site as opposed to another "non-approved" or socially irresponsible site (Griffiths, 2008). Many frauds and scams have moved into technological media such as the Internet and mobile phones. The main types of gambling fraud that currently operate on the Internet are (i) lottery scams, (ii) fake gambling site scams, (iii) betting software scams, (iv) gambling 'bonus' scams, (v) 'twofer' scams, and (vi) prize scams. These are briefly overviewed in turn.

Lottery scams: Many people receive bogus e-mails notifying them they have won a lottery (Griffiths, 2003b; Whitty and Joinson, 2009). The majority of these scams are either the 'Dutch Lottery', 'Spanish Lottery' and 'Canadian Lottery' schemes (although there are many others). The theme is always the same and they appear to make a lot of money for those that instigate the scam. According to press reports a few years ago, the Canadian Lottery scam netted over $5 billion from US victims and was making around £500,000 a month in the UK (Griffiths, 2004). Typically, a person receives an e-mail saying that they have won a lottery and they need to reply to claim their winnings (Whitty and Joinson, 2009). If the person replies, they will then receive emails, or sometimes phone calls and faxes that move the person on to the next phase of the fraud. The person will be told that they need to pay a fee - which can be variable - to cover transfer and administration costs (sometimes termed an "unlocking fee"). Sometimes the fraudsters ask for a person's bank details so that they can deposit the winnings. When this happens, the fraudsters can also steal money

directly from a person's account (Whitty and Joinson, 2008). The obvious reason why such e-mails are fraudulent is that the person has not bought a lottery ticket. However, fraudsters have started to use slightly different tactics. Below is an extract from an e-mail that I received in my inbox:

'We are pleased to inform you of the result of the Lottery Winners International programs held on the 14th of January. You have therefore been approved a sum pay out of US $500,000. CONGRATULATIONS!!! Due to mix up of some numbers and names, we ask that you keep your winning information very confidential until your claim has been processed and your prize/money remitted to you. This is part of our security protocol to avoid double claiming and unwarranted abuse of this program by some participants. All participants were selected through a computer ballot system drawn from over 200,000,000 company and 300,000,000 individual email addresses and names from all over the world.'

Here, the person appears to have had their e-mail address randomly selected into a prize draw (rather than having to have bought a ticket). To claim the prize, recipients of the e-mail are again asked to pay an administration fee. One of the more worrying aspects is that those people who have responded to these types of schemes and frauds before will find themselves named on "mooch" and "sucker" lists that are sold by specialist brokers to the fraudsters. If a person has been duped once, they will almost certainly be targeted again (Whitty and Joinson, 2009). Thankfully, there are now dedicated websites that monitor and list all known lottery scams such as those at Fraud Aid (e.g., http://www.fraudaid.com/scamspam/lottery/lottery_scam_names.htm).

Fake gambling site scams: Frauds rely on gullibility of the victim and the credibility of the criminal engaging in the fraudulent activity. On the Internet, this might perhaps translate into having very state-of-the-art webpage forgeries on the Internet with credible and trustworthy sounding materials/products (Griffiths, 2003c; Australian Competition and Consumer Commission, 2009). One of the most common fraudulent practices is when unscrupulous individuals steal materials from legitimate online gambling sites (Griffiths, 2004; McMullan and Rege, 2007). Whole website designs can be stolen including the graphics and general design. Others may just use accreditation logos from legitimate accreditation organizations such as 'GamCare' or the 'Internet Gambling Commission' (Beginners-Gambling.com, 2009). Such people rely on the fact that many gamblers have made the decision to gamble even before logging on. The urge and desire to gamble can help overcome a person's ability to think rationally and/or their instinctive mistrust of the Internet (Griffiths and Parke, 2002). Fake sites have to look safe, reputable, and trustworthy. To avoid spending money on website design and development, the fraudsters simply steal existing designs (Griffiths, 2003c). Some fake sites even go as far as making identical copies of winners' pages and testimonial pages of legitimate sites. This reinforces the idea that the site has hundreds of happy and satisfied customers. Only those who are intimately familiar with the "host" or original site would notice such a fraud.

Betting software scams: Another popular online gambling scam involves software packages that claim to identify opportunities to consistently win money by gambling (Consumer Action Law Centre, 2008; Gordon, 2009). Internet sports or casino

gambling services often require that an individual purchases software. These often involve large up-front fees and ongoing fees and charges (Australian Competition and Consumer Commission, [ACCC] 2009). This supposedly enables an individual to predict the outcome of horse races or lotteries. However, it is not possible to predict the outcome of random events such as horse races with any certainty. Betting software is often marketed by showing what an individual would have made had they invested money in the previous year (Gordon, 2009). Here, it is easy for the fraudster to demonstrate that a lot of money could have been made when they know which horse won every race. A variety of overseas lottery tickets are also marketed and sold by direct mail in many countries (ACCC, 2009). Very few are legal and fraud is often involved.

Gambling 'bonus' scams: Many online gambling sites offer incentives to get the gambler to play on their site. These include legitimate schemes such as VIP membership, loyalty schemes, and various types of deposit bonuses (i.e., the gamblers get a cash bonus if they register with the site) (Griffiths and Wood, 2008). One of the legal (but highly exploitative) ploys to get people to gamble, are those sites which require excessive play (or to have gambled a pre-set amount of money) before the cash bonus is awarded. However, there are some 'bonus' practices that go beyond exploitation and are clearly fraudulent. One of the simplest and most effective of the bonus scams is targeted at players that have been banned from a casino (Take1Look.net, 2009). Since online casinos are always in need of known paying customers, this works by drawing in banned gamblers who have moved on to other sites. The gamblers receive an e-mail offering them a cash bonus if they deposit money into their existing account. However, after the gambler has deposited the money, they do not get their bonus. The online casinos tell the player they are not eligible to receive a bonus because they were banned. Gamblers then tend to play their deposit anyway - which is exactly what the operators were hoping for. Furthermore, some online casinos cite "bonus abuse" as the reason for not paying winnings, knowing there is no governing body that can act against them (Griffiths, 2004).

The "twofer" scam: Another unscrupulous tactic is where online gambling sites that have conned a gambler once, do it again (a "two-for-one" scam) (Take1Look.net, 2009). If a gambler has signed up to a particular online casino that takes all their money and then disappears, there is little a gambler can do. Quite often, months after being ripped off, a gambler may start to get e-mails from a new gambling site set up by the fraudsters who conned the gambler in the first place (although the gambler is unlikely to know it is the same organisation). They know where to reach the gambler because of the registration form that the gambler initially filled out to join the now disbanded online casino. The fraudsters will e-mail compelling offers, rewards packages, and CD software (basically anything to get the gambler back). The fraudsters then do exactly the same again. Another variation of the 'twofer' scam is when gambling operators invite their former scammed customers (by using the information the gambler provided before at a previous site) under the ruse of 'bonuses' telling the gamblers how sympathetic they are about them being scammed, and offering a bonus if they play on their website instead (Take1Look.net, 2009).

Prize scams: Although prize scams are not gambling, they are extremely popular with fraudsters and like gambling, play on the psychology of greed. Anyone reading such a scam is promised a fabulous prize that they are guaranteed to have won (Griffiths, 2003d). All an individual has to do to claim the prize is pay a small administration fee - which they never see again. They do not get the prize either. Other prize scams include the use of pop-up windows with congratulatory messages such as *'Well done! You're today's Internet winner. Dial [telephone number] to claim your award of a holiday/television/car!!!'* The pop-up is basically an advertisement as the 'prize' is usually a worthless discount voucher or similar (Griffiths, 2003d).

Online gamblers: A target for cyber-criminals

It is also worth noting that Internet gamblers themselves may become victims of other cybercrimes. For instance, gamblers (playing in places like online casinos) may be targeted by criminals who try to steal money from them by infecting their computers (Sturgeon, 2006). It is certainly the case that Internet users who have financial transaction data are attractive targets for criminals. In these cases, criminals may use a 'raketracker' tool that allows users to monitor the house's take on their games. Using the tool, the criminal can access login details for a variety of well know online casinos. The criminals can then make money by setting up games between themselves and the compromised online gamblers (Sturgeon, 2006). Another way in which Internet gamblers may be targeted is via those who play online poker. Here, it is possible for online poker players to be competing against a 'poker bot' (a computer programme that plays poker against a real human opponent) without the player being aware. However, it should be noted that a recent overview on poker bots concluded that at present, poker bots are not technically illegal in most jurisdictions although this may change (Griffiths, 2009).

Concluding comments

In this short paper it has been shown that technology is being used to exploit and defraud thousands of people. One of the specific downsides of gambling fraud on the Internet, and cyber-crime more generally, is that much of the crime is potentially global if carried out on the Internet. However, cross-border investigations are the rarity and there are often only weak extradition treaties. This means that there are many international cyber-criminals who simply do not get caught and/or do not reach the courts. There is also the issue of regulatory intervention. It is only recently that regulators have begun to take Internet crime seriously but the authorities are struggling to keep pace with criminals who have technological expertise. Consumer associations across the world are united that there should be internationally agreed minimum standards of truthfulness and accountability on Internet websites and that governments should enforce these. They want to see internationally agreed mechanisms that can help in the protection of the consumer engaged in e-commerce. Clearly, bringing cyber-criminals to justice can be hard but the situation does appear to be changing with many more countries putting cyber-crime higher up the priority agenda.

It is also worth noting that there appears to be one major reason why gambling is such a growth area for fraud. This is the fact that many gamblers themselves want to get a huge reward from a small outlay (just as the fraudsters do). As long as there are people who are prepared to risk money on chance events, there will be those out there who will want to fraudulently take their money from them. To date, there is almost no empirical data on any of these criminal practices and it is hard to assess the extent to how widespread any of these fraudulent online gambling practices are. There is clearly a need to examine this area empirically and for research to be initiated in this newly emerging area of criminological concern.

References

Australian Competition and Consumer Commission (2009) Sports 'investment' scams [online]. Available from: http://www.accc.gov.au/ [Accessed: 27/11/2009].

Beginners-Gambling.com (2009) How to avoid online gambling scams [online]. Available from: http://www.beginners-gambling.com/ [Accessed: 27/11/2009].

Consumer Action Law Centre (2008) Dodgy First Choice betting software scam should be your last choice (Media Release) [online]. Available from: http://www.consumeraction.org.au/ [Accessed: 27/11/2009].

Excell, D. (2009) Spotting a fraudster's 'tell': Catching online gambling cheats through behavior patterns [online]. Available from: http://www.kroll.com/about/library/fraud/Jun2009/catching_gambling_cheats.aspx [Accessed: 27/11/2009].

Gordon, C. (2009) Sports betting strategy software - Looking to make big money? *EzineArticles.com.* June 10 [online]. Available from: http://ezinearticles.com/?Sports--Betting--Strategy--Software------Looking--to--Make--Big--Money?andid=2461445 [Accessed: 27/11/2009].

Griffiths, M.D. (1994) Beating the fruit machine: Systems and ploys both legal and illegal. *Journal of Gambling Studies*, 10, 287-292.

Griffiths, M.D. (2000) Internet gambling and crime. *Police Journal,* 73, 25-30.

Griffiths, M.D. (2003a) Internet gambling: Issues, concerns and recommendations. *CyberPsychology and Behavior*, 6, 557-568.

Griffiths, M.D. (2003b) Dot cons: Exploitation and fraud on the Internet (Part 2). *The Criminal Lawyer*, 134, 3-5.

Griffiths, M.D. (2003c) Exploitation and fraud on the Internet: Some common practices, *The Criminal Lawyer*, 132, 5-7.

Griffiths, M.D. (2003d) Dot cons: Exploitation and Fraud on the Internet (Part 2). *The Criminal Lawyer*, 134, 3-5.

Griffiths, M.D. (2004) Hi-tech gambling scams. *The Criminal Lawyer*, 140, 4-5.

Griffiths, M.D. (2006) An overview of pathological gambling. In T. Plante (Ed.), *Mental Disorders of the New Millennium. Vol. I: Behavioral Issues.* 73-98. New York: Greenwood.

Griffiths, M.D. (2008) Online trust and Internet gambling. *World Online Gambling Law Report,* 8(4), 14-16.

Griffiths, M.D. (2009) Are poker bots really a criminal issue? *E-Commerce, Law and Policy*, 11(5), 12-13.

Griffiths, M.D. and Hopkins, M. (2001) Betting shop violence: A cause for concern? *Police Journal,* 74, 55-60.

Griffiths, M.D. and Parke, J. (2002) The social impact of internet gambling. *Social Science Computer Review*, 20, 312-320.

Griffiths, M.D., Parke, A. and Parke, J. (2005) Gambling-related violence: An issue for the police? *Police Journal,* 78, 223-227.

Griffiths, M.D. and Sparrow, P. (1996) Funding fruit machine addiction: The hidden crime. *Probation Journal,* 43, 211-213.

Griffiths, M.D. and Wood, R.T.A. (2008) Gambling loyalty schemes: Treading a fine line? *Casino and Gaming International,* 4(2), 105-108.

McMullan, J. and Rege, A. (2007) Cyberextortion at online gambling sites: Criminal organization and legal challenges. *Gaming Law Review*, 11, 648-665.

Parke, A., and Griffiths, M.D. (2004) Aggressive behavior in slot machine gamblers: A preliminary observational study. *Psychological Reports*, 95, 109-114.

Smith, G., Wynne, H. and Hartnagel, T. (2003) *Examining police records to assess gambling impacts: a study of gambling-related crime in the city of Edmonton.* Report for the Alberta Gaming Research Institute.

Sturgeon, W. (2006) Tech's big gamble. Online casino punters targeted by malware scams. Silicon. Com, May 17 [online]. Available from: http://www.silicon.com/research/specialreports/gambling/0,3800010160,39158950,00.htm [Accessed: 27/11/2009].

Take1Look.net (2009) Online gambling scams: How to avoid them [online]. Available from: http://www.take1look.net/online-gambling-scams.html [Accessed: 27/11/2009].

Whitty, M. and Joinson, A. (2009) *Truth, Lies and Trust on The Internet.* Hove: Routledge.

Yeoman, T. and Griffiths, M.D. (1996) Adolescent machine gambling and crime. *Journal of Adolescence*, 19, 183-188.