The challenges of countering fraud in Malta's remote gaming industry

ZERAFA, Antonio, BANKS, James <http://orcid.org/0000-0002-1899-9057> and WATERS, Jaime

Published version

ZERAFA, Antonio, BANKS, James and WATERS, Jaime (2021). The challenges of countering fraud in Malta's remote gaming industry. Journal of Financial Crime.

The challenges of countering fraud in Malta's remote gaming industry

Introduction

Gambling's association with trickery, cheating and fraud has a long lineage, far predating the emergence of the internet as a medium for wagering activities. Indeed, gambling itself has been invariably portrayed as both a criminal and criminogenic activity (Morse and Goss, 2007). Across the globe, jurisdictions have endeavoured to regulate gambling, in order to prevent crime and disorder. Thus, as opportunities for gambling have proliferated, states and a global commercial gambling industry have sought to institute laws, policies and processes that minimise the risk of fraud and other forms of criminal activity (Banks and Waugh, 2019). Yet the development of the internet as a commercial and public vehicle that provides many citizens of world with unfettered access to wagering activities presents new and significant challenges to those charged with ensuring gambling's continued governance, security and profit.

This paper explores the challenges of countering fraud in Malta's remote gaming[1] industry. By way of introduction, the paper provides a brief overview of the development of online gaming, before summarising previous academic literature focused on the interrelationships between online gambling and crime. Discussion then turns to explore the nature of fraud in Malta's remote gaming industry and the challenges associated with reporting and responding to online gambling related fraud. Data is derived from semi-structured interviews with key personnel working in regulatory roles within the sector.

[1] The terms gambling and gaming are often used interchangeably. Gaming is favoured by the industry, as it is more associated with play and leisure.

Consequently, this paper offers rare and unique insight into crime threats pertaining to the remote gaming industry in Malta that is likely to have international applicability.

The development of remote gambling

In little over two decades, remote gambling has developed into a heterogenous, highly accessible and increasingly complex marketplace worth in excess of US$23 billion (H2 Gambling Capital, 2015). Comprising of 3,500 gambling sites located across 70 different countries, global gamblers have access to a panoply of online casinos, sports books, bingo sites, poker rooms, lotteries, fantasy sports operators, skill game sites, betting exchanges, and forex and binary trading sites (Casino City, 2019). It is unsurprising then that international studies (Williams and Wood, 2009; Wardle et al., 2011; Gainsbury, 2012) indicate that between 1 and 30 per cent of adults have gambled remotely, with internet gambling representing the fastest growing segment of the industry (Global Market Insights, 2020). Remote gambling is forecast to continue to exhibit an upward trend in terms of participation rates, industry profits and state taxation revenues, as new markets emerge and states open up their markets to competition (Ibid.).

The Republic of Malta is emblematic of the success of remote gambling across many countries of the world. Despite being the European Union's smallest member state in terms of territory and population, Malta has emerged as one of principal destinations for remote gaming businesses. Quick to respond to the evolution of the internet as a new medium for gambling, in 2004 Malta became the first European Union member state to endorse across-the-board legislation on remote gaming. By 2017, the gaming sector had established itself as the country's third largest industry, contributing between 10-12% of Malta's Gross Domestic Product (GDP) (Malta Gaming Authority, 2018). In total, 294 gaming companies are located

in Malta, whilst 625 remote gaming licenses have been issued. As a consequence of Malta's favourable tax regime, as of 2019, the country is now home to many of the remote gaming industry's leading operators, including Unibet, Tipico, Betsson, Paddy Power, Betfair, bet365, and DraftKings (Strickland Jr., Zammit, Portanier & Baron, 2019). Consequently, Malta generates approximately €60m in gaming tax revenues, whilst the industry employs 6,673 full-time staff (Malta Gaming Authority, 2018).

Given the marked growth of remote gaming in Malta, the significant sums of money held in online accounts and flowing between gambling operators and myriad ancillary organisations, it is unsurprising that the industry is attractive to criminals. The criminal activities associated with remote gaming are vast, can be high-tech in nature and involve a variety of different methods that continue to evolve over time (Zerafa, 2016). This is evidenced by a growing number of studies which have examined gambling and crime in virtual environments, and are considered in the next section of this article.

Previous Literature on Gambling and Crime

Whilst the manifold actual, possible, and probable interconnections between gambling and crime have been well-established, the relationship between the two has altered significantly, as consequence of the advent of the internet and the evolution of digital media and information communication technologies. In response, a small but developing body of academic literature has examined the interrelationships between online gambling and crime (McMullan and Rege, 2007, 2010, 2012; McMullan, 2012; Banks 2012, 2013, 2014; Zerafa, 2016; Banks, 2017). Collectively, these studies demonstrate several crime threats and problems that may impact remote gambling operators, their customers and wider society. This includes illegal and underage internet gambling, cyber-extortion and (distributed) denial

of service attacks (DDoS), money laundering and terrorist financing, gambling-related crime, match fixing, and theft and fraud.

Crimes relating to remote gambling may be committed by a range of different groups and individuals. For Banks (2012: 3), the remote gambling environment is a 'contested space' in which site operators, employees, customers and 'unwanted third parties' may interact. Such intermingling creates 'opportunities for multi-various forms of criminal activity and [the construction of] rhizomatic relations between perpetrators and victims' (Ibid.). McMullan and Rege's (2010) web-based analysis of crimes that have occurred in and around remote gambling sites suggests that online offenders engaged in acts of extortion, theft and fraud range from solo actors to amorphous and loosely connected criminal assemblages. McMullan and Rege's typology posits three distinct categories of 'virtual villain'. First, 'cybernomads' consist of solo actors who typically purchase or construct digital 'toolkits' that allow individuals to steal or defraud remote gambling businesses and their customers. More sophisticated 'professional' cybernomads may write malware or steal and sell gambling site customers' personal information. Second, small-scale organised crime groups or 'dot.con teams' involve a range of individuals, including players, gambling site owners, managers and employees, software developers, and consultants who work together to commit acts of money laundering, fraud or theft. Third, the most sophisticated 'criminal assemblages' consist of dynamic and complex professional criminal networks who continuously engage in money laundering, phishing, fraud and extortion activities.

Fraud and theft that occurs at or around online gambling sites is a particular concern for legitimate gambling operators and their clientele. Such crimes can impact the playing experience, undermine the reputation of online gambling, and reduce operators' ability to retain the custom of existing players and recruit new ones (Banks, 2014). Indeed, a lack of trust in payment processes, site security and the legitimacy of operators are cited as principal

reasons why some citizens do not gamble online (Ipsos Reid, 2005; Wood and Williams, 2010; Gainsbury, Parke and Suhonen, 2013). For example, one-third of 12,000 respondents to a worldwide survey on internet gambling, recognised the difficulty in verifying the fairness of games, while over twenty-five per cent expressed concerns regarding the safety of the money deposited at sites (Williams and Wood, 2010). Elsewhere, a study by the American Gaming Association (2006) noted that over half (55%) of internet casino gamblers surveyed believed that they were cheated by site operators. Parke et al.'s (2007: 14) survey of 10,000 online gamblers delivered a similar finding, with the survey authors noting that:

> Levels of mistrust and cynicism are epitomised by the fact that only half of respondents felt that online gambling software was fair and random, and in fact, over a third of respondents thought there was an "on/off switch that could turn the software in favour of the operator". Consequently, ensuring that websites are safe and secure, games are fair and businesses are operated with integrity is essential if online gambling is to sustain.

Two principal types of fraud impacting the remote gaming industry are discernible , and although the profit motive remains the same, they typically operate in a distinct manner. Internal fraud involves organisation insiders, such as gambling site owners, operators, or other personnel, who defraud the gambling company or its customers. External fraud involves players or 'criminal entrepreneurs' who target sites and/ or their clientele. Whilst Zerafa (2016) suggests that external forms of fraud are more prevalent, two of the most celebrated frauds which occurred at the height of the online poker boom involved gambling insiders. The superuser scandals involving Absolute Poker and UltimateBet – two of the then leading

online operators – caused widespread consternation amongst internet gambling communities, leaving a legacy of distrust amongst players. Indeed, Woods and Griffiths (2008: 90) note that:

> There was a lot of suspicion amongst the professional players that sometimes they were playing against computer programs (bots), particularly when they lost. Similarly, there was fear amongst some that certain computer viruses could be used by another player that would allow them to see other players' cards. Talking to other players using the chat facility was one way that a player could be sure that they were in fact playing with real people.

As detailed above, research evidence gathered from gamers and open access materials suggests that fraud relating to online gambling is a notable issue of concern for the industry. However, to date, no study has reported on the views and experiences of gaming operators and regulators. In response, this qualitative research study considers data derived from interviews with professionals and stakeholders from Malta's remote gaming industry to provide new insights into crime and online gambling. The methodological approach employed in this study is discussed below.

Method

Six individuals from three major stakeholders in Malta's remote gaming industry were interviewed for this study. Ethical approval was granted by the University of [Name Anonymised]. The study was submitted to the [Name Anonymised] Ethics Committee, in line with policy and associated procedures that are applied to all research undertaken under the

auspices of the University. All participants were given information regarding the research and gave full consent to participate in the interviews.

To date, research studies pertaining to the topic of crime in the remote gaming industry that incorporate the perspectives of gambling operators and regulators are scarce (a notable exception is the work of Brooks (2012) who interviewed five gambling operator personnel for his study on money laundering). This is undoubtedly a consequence of the reputational and commercial imperatives that impact the degree to which gambling businesses and those charged with their governance are willing to participate in academic research. In addition, access to potential research participants may be challenging for researchers who are situated outside of the gambling industry. Thus, whilst gambling operators and regulators may not be consider 'hard to reach' research subjects as defined by the research methods literature, they can be difficult to access for those researchers who do not have the requisite personal contacts or links to 'gatekeepers'.

This study's originality is, in part, because data has been gathered from key stakeholders working in one of the world's largest remote gaming industries. This was achieved through the first author's role within the Malta Gaming Authority (MGA) which enabled him to recruit research participants from across the sector. Table 1 details the characteristics of the interviewees; the organisation they work for, the department in which they work, and an overview of their duties. The research study sought to generate a holistic understanding of the challenges of countering fraud in Malta's remote gaming market through the unique perspectives of professionals working for the three key industry stakeholders; the MGA, Malta's police force, and licensed remote gaming operators. As such, although the research sample is small, it includes key individuals working within the MGA (including Information Computer Technology (ICT) & Records Department, Enforcement Directorate, Player Support Department, Legal Department), the Economic Crime Unit of the

Malta Police Force, and the Fraud Department of a Malta Licensed Remote Gaming Operator.

[INSERT TABLE 1 HERE]

Interviews were conducted by the first author either at the interviewees' place of work or at a mutually convenient location. The interviews were semi-structured in nature, in order to gather a breadth and depth of qualitative data regarding fraud in Malta's remote gaming industry. Such an approach enabled the interviewees to detail their own experiences and opinions regarding the challenges of identifying, preventing, and responding to criminal activity, and enabled the interviewer to probe for further information regarding some of the issues raised. Interviews took between 60 and 120 minutes and were audio recorded.

Interviews were transcribed and, where necessary, translated into English. The transcripts were explored using an interpretive thematic analysis (Braun and Clarke, 2006). After familiarising ourselves with the data through preliminary readings, the research team undertook line-by-line coding, formulating initial category and sub-category codes. Codes were then categorised into a smaller number of themes, in accordance with their semantic meaning. This analytical approach enabled the initial categories to be reduced to a smaller number of themes. It is these themes that structure the results section below, wherein quotes from the interviews are employed to support the presented analysis.

Research Findings

Research findings are divided into two sections. First, the forms, features and organisational dynamics of frauds committed in and around Malta's remote gaming industry are explored. Second, the potential reasons for the underreporting of such offences are examined.

The forms and features of fraud in Malta's remote gaming industry

In Malta, as in other jurisdictions across the globe, online gambling is seen as a 'place' in which consumers can engage in a range of 'safe' aleatory activities. However, the geographical indeterminacy of the internet, coupled with the limitations of state-based law and the itinerant nature of web sites, means that opportunities for criminal enterprise present themselves in the online gambling arena. All interviewees agreed that fraud presents the principal crime challenge to Malta's remote gaming industry, though it manifests itself in diverse ways and encompasses various other sub-categories of crime. For example, the research participant who works in the MGA Enforcement Directorate noted that fraud may be committed by a variety of different groups and individuals involved with the remote gaming sector and encompass a range of acts:

> [F]raud is one of the most common crimes found in remote gaming. However, it can take various forms. The fraud could be from the player's side, it can be from the employer himself or the remote gaming company's employees who defraud the game itself; and also other forms of crimes where indirectly there will be fraud, for example match fixing.

All participants suggested that identity-related crimes are the most common type of fraud that take place crime in Malta's remote gaming industry. Operators may receive tampered

documentation or uncover players who are using the identification cards or utility bills of others. Whilst such an approach may be employed for the purposes of money laundering (Levi, 2009), the participants from the MGA's Legal Department suggested that bonus abuse is the principal reason why individuals may create multiple aliases and forge or misappropriate documentation:

> When you have an operation that is of low transaction value, that is where you need a high number of transactions, where profit is based a lot on customer acquisition and retention, and therefore there are a lot of bonuses and other incentives on offer to the players, one of the most [common] frauds that has developed online is the possibility of an individual abusing the introductory bonuses awarded by creating multiple identities and opening new accounts.

Such an approach can be a highly lucrative criminal venture. For example, in the UK, Andre Ospiau was jailed for three years for amassing around £80,000 from bonus related fraud involving 5,900 passports, identity cards, bills and associated documentation (Garlitos, 2012). Whilst research participants recognised that preventing the opening of multiple accounts by a single individual can prove challenging, Know Your Customer (KYC) processes are often effective in identifying cases of identity fraud.

KYC processes are also key to uncovering credit card fraud involving bank card and pin details which have been stolen and sold online. Examining claims that credit cards have been used fraudulently is a regular activity of gambling operators and can prove challenging. The research participant working in the Fraud Department of an online gaming operator suggests that the illegal use of credit card information is commonplace:

> This information is very easily accessible. That is if you require stolen credit cards - in a flash you can get a spreadsheet with all the details and you can use them the way you want. Because a lot of people see it [(gambling)] as easy money, but remote gaming is a risk. If you are going to play a game…you can lose your money but potentially you can win. Therefore, they will eliminate the risk and use other people's money. If it comes good, it's good, if it goes wrong, they don't lose anything, they have just spent an hour [of their] time [playing]. That's the mentality.

The participant goes on to note that often in such cases the victim has no relationship with either the operator or the individual playing on the operator's website. By contrast, the interviewee working in the MGA's Player Support Department notes that claims of credit card fraud are frequently unproven, with evidence indicating that it is the owner of the card who has gambled and then fraudulently lied about their card's misuse in an attempt to recoup their losses.

Other common player behaviours include chip dumping[2] and collusion[3] between multiple players at the table. The research participant from the Fraud Department noted that whilst the dumping of large amounts of money for money laundering purposes is easy to identify, collusion at a table that finishes with the dumping or losing of chips to the 'chip leader' is much harder to identify, as effective automated processes are yet to be devised:

[2] Chip dumping is a strategy whereby one player deliberately loses their poker chips to another. Such an approach may feature in cash games as part of coordinated play between two or more players in order to launder money.
[3] This typically involves two or more players coordinating their play so as to defraud other players.

> Where you have chip-dumping you have to see it yourself. You have to analyse the game, you have to see when the move of the chip-dumping took place. As soon as a game finishes [the hand history] is available as a document to the agent. That need to be 'hands on'. It is very much subject to interpretation. It is difficult to automate it.

Coordinated play, particularly where it is supported by technology such as bots[4], can be highly lucrative. For example, players at PokerStars were defrauded of approximately US$1.5 million at fifty cent, one dollar and two dollar pot limit Omaha tables by a team of players primarily from Russia and Kazakhstan (Glatzer, 2015).

Whilst the primary forms of fraud detailed above are not contingent on any technological competence, other forms of fraud require the offender to be able to modify digital data. For example, unlicensed websites may adopt the MGA's logo or detail that they are licensed by them on their site. As Banks (2017: 205) notes, unlicensed sites use 'fake kite marks of social responsibility…to indicate that they hold an appropriate operating licence, are accredited by an independent third party or subject to regulatory oversight and dispute resolution procedures.'. In addition, as the research participant from the Information Computer Technology and Records Department highlights, an unlicensed operator may use vague references to the MGA in order to indicate that their site is legitimate, whilst seeking to hide its online presence from the regulator:

[4] A bot is a computer program that performs automated tasks. For example, a poker bot is a computerised poker player that is programmed to play hands of poker.

> [W]e frequently find that there are operators who state that they are licensed by us, and they write it somewhere in the terms and conditions; hidden, so that we, as regulators, would not find it so easily. They state that their jackpot is licensed by "the Maltese regulator" instead of by the "Malta Gaming Authority", so that if anyone intentionally searched for the term in Google, they wouldn't be able to find it.

Other fraudsters may reproduce games that belong to other operators or 'lift' aspects of a site's design or content. Such forgeries can dupe unsuspecting customers into depositing money and wagering it at unlicensed sites which fail to pay any winnings to players.

In addition to the principal forms of fraud detailed above, our participants made reference to the alteration of games, 'taking-over' of accounts, and distributed denial of service attacks which had resulted from the actions of more technically skilled fraudsters. Collectively, the crimes detailed by our interviewees demonstrate that the types and techniques of fraud committed at or around online gaming sites regulated by the MGA are numerous. Despite this, reported offences remain low. The next section explores the reasons why such crimes are underreported, the implications for effective regulation and intervention, and potential remedies.

The reporting of fraud

Despite recognition by our participants that fraud is a perennial problem in Malta's remote gaming industry, there is little by way of data regarding the extent of such crimes. The principal source of data is the annual report issued by the Financial Intelligence Analysis Unit

(FIAU) in Malta. The report documents the number of 'Suspicious Transaction Reports'[5] (STRs) received by the FIAU from a range of financial institutions including remote gaming operators over the previous year. Evidence indicates a notable growth in the number of STRs filed by remote gaming companies, rising from 87 in 2016 to 218 in 2017, to 724 in 2018, and to 1445 in 2019. In 2019, 52% of STRs received by the FIAU were filed by remote gaming companies, with fraud representing 'the most prevalent suspected predicate offence' with 596 instances reported across all STRs (Financial Intelligence Analysis Unit, 2020: 34). However, the number of reported STRs still remains low, given that the gaming industry in Malta comprises of approximately 300 operators holding in excess of 600 gaming licences. Our participants indicated that many incidents of fraud go unreported and unrecorded, and that this stems from a number of factors.

A notable concern of operators is that the frequent reporting of potential cases of fraud may damage their reputation with the regulator, lead to greater oversight and scrutiny, and have implications for the renewal of their licence. As the research participant working in the ICT & Records Department notes: 'I think that there are some operators that don't even report [cases of fraud] in the first place so that they do not become a concern of the regulator'. To resolve the situation, some customers who are victims of fraud are simply 'paid off'. For example, the member of staff from the Player Support Department at the MGA highlights how:

> [M]any operators would not want the case to end up with us, for the simple reason that it could attract unnecessary or unwanted attention. Maybe it will lead

[5] Suspicious Transaction Reports can relate to a variety of potential offences including: corruption and bribery, fraud, illegal gambling, illicit trafficking in narcotic drugs and psychotropic substances, insider trading and market manipulation, participation in an organised criminal group and racketeering, tax offences, and terrorism including financing terrorism,

> to the MGA investigating them in some way. I believe that this is what most [operators] would say. There are some of them that say, "I don't want the complaints at MGA full stop, so just pay the player off, close the account and he will not come again". Some do it for the sake of expediency. The operator just pays and moves on.

Whilst reimbursing the player may represent one mechanism through which operators can resolve a case where fraud is alleged, such an outcome may only be warranted after detailed investigation. Indeed, the participant from an online gaming operator's Fraud Department suggests that one of the reasons for the underreporting of such offences by operators is that they deem themselves, at least in the first instance, best placed to investigate potential frauds. For example, our interviewee notes how in cases where players suggest that they have been the victim of fraud: 'We never escalate it, because we deal with it at source. We do research. Often the player has broken the terms and conditions [of wagering with us]. I don't need to escalate such cases'. The staff member noted that remote gaming operators have an array of reliable systems that allow them to investigate the crime of fraud 'in-house' and hence be able to determine whether a client is being fraudulent or not. In addition, certain operators are capable of identifying a player's current location, his or her gaming patterns, and his or her possible relationships with 'clients of concern' that have, or have attempted to, previously circumnavigate or corrupt their site's systems or processes.

Compounding this perspective is the inability of the MGA as regulator and Malta Police Force to solve or resolve some crimes committed against operators. The member of staff from the Player Support Department at the MGA suggests that in some cases 'if, for example, we take a DDoS, some offenders are never caught…they mask their IP, use proxies properly. There are those who are very capable of hiding their identity and location, and are

not caught.' Moreover, it is suggested that the 'fissured structure of law enforcement within and between nation states' (McMullan and Rege, 2007: 659) undermines attempts to address cybercrimes such as fraud where they cross national boundaries. Such challenges are compounded by the slow development of technical knowledge and competence, alongside limited resources, which mean that police forces are unable to collect evidence, trace, apprehend and eventually prosecute online offenders. As such reporting potential offences of fraud are deemed by operators to be costly, time consuming and unfruitful.

Whilst many offences committed by fraudsters against online gaming operators may go unreported, the research participant at Malta Gaming Authority's Enforcement Directorate suggests that 'high value' offences are always reported to the unit for investigation: '[M]any companies are quite reluctant to report [incidents of fraud], but they have bench marks. So if you have a case that involves more than X amount [of money] they will report it, otherwise they try to avoid it.' This is reinforced by the Officer at Malta Police Force's Economic Crime Unit who notes that whilst online gaming operators' commercial imperatives mean that they will seek to avoid public scrutiny where possible, they will report monetarily sizeable incidents of fraud:

> when [the] criminal activity impacts the remote gaming operator in a way and manner where the losses incurred are substantial, or when the criminal activity gives rise to certain legal and/or jurisdictional issues that only the Malta Police Force would have the legal capabilities to deal with.

The officer goes on to state that regular and consistent reporting by operators, and a willingness to share information, would benefit operators and Malta's remote gaming

industry more broadly. Such a viewpoint is echoed by the research participant from MGA's Enforcement Directorate who notes that information sharing depends on operators utilising reporting processes. The interviewee further highlights how remote gaming operators reporting of incidents of fraud will enable the organised compilation of intelligence which can later be shared with a view to enhancing operator and regulators' approaches to crime prevention:

> It is worth reporting the crime even if the operator or player are not going to gain anything. For what reason? The reason is that by collecting these type of reports, the authorities will be building intelligence. […] Yes, the victim can say I am not going to gain anything in the short term if I report it to the Malta Police Force. But to the authorities this information is of great use in preventing other operators becoming a victim.

Moreover, the participant explains that this intelligence would allow the industry to better evaluate the illicit methods adopted by fraudsters. This information may then be communicated to institutions such as Europol, in order to facilitate the sharing of information across European Union member countries. Thus, whilst a remote gaming operator may not find any immediate and direct benefit to reporting incidents of fraud, the report could contribute to reducing such crimes in remote gaming in the future. This sense of collectiveness was echoed by other research participants who suggested that it is only by gaming operators working together, sharing data and reporting incidents of (potential) crime to regulators that the remote gaming industry can further its fight against fraud.

Conclusion

This study's originality stems from data gathered from six individuals working at three principal stakeholders in Malta's remote gaming industry. Academic studies that engage gambling operators and regulators are rare, given the commercial and reputational sensitivities that inhibit their willingness to partake in such research. This study offers insight into the extent and nature of fraud in and around online gambling sites. Our participants suggest that fraud is a perennial problem for the industry, with gamblers, operators, and members of the general public victims of gambling-related offences. The forms and organisational dynamics of fraud vary, but principal offences relate to credit card and identity fraud, collusion, and account takeover. Evidence also indicates that although the number of offences reported by the gaming industry continues to grow, many cases of fraud go unreported and unrecorded. The interviewees highlight how online gaming operators' failure to reports incidents of fraud stem from several interrelated reasons. In particular, operators may be concerned about the reputational damage that may result from incidents of fraud in and around their websites, as well as coming under increased scrutiny from their regulator. Increased reporting may also lead to a loss of public confidence in the safety and security of a company's gaming website, resulting in reduced uptake by new players and the retention of existing customers. Additionally, participants advocate that operators may see themselves as best placed to investigate potential cases of fraud, particularly as liaising with regulators and law enforcement agencies can be resource intensive and not lead to a satisfactory outcome.

Overcoming operator concerns and encouraging a culture of reporting and information sharing is paramount, if regulators, law enforcement agencies and operators are to prevent and effectively investigate incidents of fraud. Whilst our participants indicate that there is a 'tipping' point' where cases of fraud that might cost the operator notable sums of money will be reported, it is essential that all fraudulent activities are reported to and

recorded by regulators. Though many of these reports may not lead to a successful investigation, a culture of regular reporting will facilitate a stable system of information sharing, underpinning a holistic intelligence gathering process. Such a process will enable greater insight into and understanding of the evolving organisational dynamics of fraudulent practices in and around the online gaming industry, and enable law enforcement agencies, regulators and operators to develop, institute and enhance mechanisms and processes through which to combat such offences.

References

American Gaming Association. 2006. 2006 State of States: The American Gaming Association survey of casino entertainment. htttp://www.americangaminngorg/survey2006/reference/ref.html.

Banks, J. (2012). Online Gambling and Crime: A Sure Bet? The ETHICOMP Journal.

Banks, James. 2013. Edging your bets: Advantage play, gambling, crime and victimisation. Crime, Media, Culture 9: 171-187.

Banks, James. 2014. Online gambling and crime: Causes, controls and controversies. London: Ashgate.

Banks, James. 2017. Gambling, crime and society. London: Palgrave MacMillan.

Banks, James, and Dan Waugh. 2019. A taxonomy of gambling-related crime. International Gambling Studies 19: 339-357.

Braun, V. and Clarke, V. (2006) Using thematic analysis in psychology. Qualitative Research in Psychology, 3 (2). pp. 77-101.

Brooks, Graham. 2012. Online gambling and money laundering: 'Views from the inside'. Journal of Money Laundering Control 15: 304–315.

Casino City. 2019. Online casino city, http://onlinecasinocity.com. 20 May 2020.

Financial Intelligence Analysis Unit. 2020. Annual Report 2019. Malta: Financial Intelligence Analysis Unit.

Gainsbury, S. 2012. Internet gambling: Current research findings and implications. New York: Springer.

Gainsbury, S. Parke, J. and Suhonen, N. 2013. Consumer attitudes towards internet gambling: Perceptions of responsible gambling policies, consumer protection, and regulation of online gambling sites. Computers in Human Behaviour, 29: 235-245.

Garlitos, K. 2012. Sportsbook bonus abuser gets sent to jail for three years. CalvinAyre.com [online] 11 April. https://calvinayre.com/2012/04/11/business/sportsbook-bonus-abuser-gets-sent-to-jail-for-three-years/

Glatzer, J. 2015. Pokerstars and players react to pot-limit Omaha bot scandal. Pokernews [online] 18 June. https://www.chatsports.com/poker/a/source/pokerstars-and-players-react-to-pot-limit-omaha-bot-scandal-11522591

Global Market Insights. 2020. Industry Trends. https://www.gminsights.com/industry-analysis/online-gambling-market

H2 Gambling Capital. 2015. eGaming Data Bulletin. www.h2gc.com. 11 November 2020.

IPSOS Reid, 2005. Online Poker in North America: A syndicated study. http:www.ipsos-na.com

Levi, Michael. 2009. Money-laundering risks and e-gaming: A European overview and assessment. Final Report. Cardiff: Cardiff University.

Malta Gaming Authority. (2018). The Malta Gaming Authority Annual Report 2017. Retrieved from http://mga.org.mt/consultations-publications/

McMullan, L. John. 2012. Cyber fraud, online poker and order-maintenance in virtual worlds. Gaming Law Review and Economics 16: 100–113.

McMullan, L. John, and Aunshul Rege. 2007. Cyber-extortion at online gambling sites: Criminal organisation and legal challenges. Gaming Law Review 11: 648–665.

McMullan, J.L., & Rege, A. (2010). Online Crime & Internet Gambling. Journal of Gambling Issues, No. 24.

McMullan, L. John, and Aunshul Rege. 2012. Internet gambling and online crime. In Routledge international handbook of internet gambling. Edited by Robert. J. Williams, Robert. T. Wood, and Jonathan Parke, 331–348. London: Routledge.

Morse, E.A. and Goss, E.P., 2007. Governing fortune: Casino gambling in America. Michigan: University of Michigan.

Parke, J. Rigbye, J.L. Parke, A.J. and Vaughan-Williams, L. 2007. The eCOGRA global online gambler report. London: eCOGRA.

Strickland Jr., R., Zammit, M., Portanier, R., & Baron, K. (2019). Gaming Jurisdiction Overview: A New World of Possibilities. Gaming Malta: 2019 Edition, 10-19. Retrieved from https://issuu.com/countryprofilermaltaltd/docs/gaming-2019

Wardle, H., Moody, A., Spence, S., et al., (2011). British gambling prevalence survey 2010. London: National Centre for Social Research.

Williams, R.J. & Wood, R.T. (2007). Internet Gambling: A Comprehensive Review and Synthesis of the Literature. Report prepared for the Ontario Problem Gambling Research Centre, Guelph, ON.

Wood, R.T. and Griffiths, M.D. 2008. Why Swedish people play online poker and factors that can increase or decrease trust in poker websites: A qualitative investigation. Journal of Gambling Issues, 21: 80-97.

Wood, R.T. and Williams, R.J. 2010. Internet gambling: Prevalence, patterns, problems and policy options. Final report prepared for the Ontario Problem Gambling Research Centre, Guelph, Ontario, Canada.

Zerafa, A. (2016). Online Gambling & Crime: An Indissoluble Relationship. University of Malta

Table 1: Characteristics of the research sample			
Participant	Organisation	Department	Duties
Participant 1	Malta Gaming Authority	Information Computer Technology (ICT) & Records Department	The MAG ICT and Records Department is responsible for: IT administration; systems maintenance and ongoing development; technology and infrastructure planning; IT security; implementation and maintenance of the Authority's CRM system; management of the information systems in general. The department is also charged with the archiving, scanning, and registration of documentation that is in the Authority's possession.
Participant 2	Malta Gaming Authority	Enforcement Directorate	The Enforcement Directorate is responsible for: field inspections in Malta's land-based gambling outlets; ensuring compliance; criminal probity vetting; on-site visits to review Anti-Money Laundering (AML) policies and procedures; following up on intelligence reports in order to conduct investigations into land-based and remote operations.
Participant 3	Malta Gaming Authority	Player Support Department	The Player Support Department manages complaints emanating from players engaged with one or more of MGA's licensed operators and resolves any disputes that result from Business-to-Customer relationships.

Participant 4	Malta Gaming Authority	Legal Department	The Legal Department oversees the MGA's legal affairs: reviewing and drafting internal and external contracts; providing legal advice; representing the Authority during Court sittings; liaising with the Attorney General's office; reviewing legislation; public consultations; the implementation and development of policy
Participant 5	Malta Police Force	Economic Crime Unit	The Economic Crime Unit is charged with investigating crimes such as: fraud, misappropriation, forgery, and embezzlement; bounced, stolen, and forged cheques; plastic card fraud; foreign counterfeit currency; usury; intellectual property right infringements; VAT fraud and misappropriation cases; computer and internet fraud; extortion, money laundering, and other related crimes
Participant 6	Malta Licensed Remote Gaming Operator	Fraud Department	The Fraud Department provides: key operational metrics and statistics relating to the playing patterns of players; establishes and manages payments made by players; seeks to detect any fraudulent activities by players. This research participant is an expert in the field of fraud in remote gaming having focused his post-graduate studies on the subject matter, alongside over ten years-experience of working in Fraud Departments for some of Malta's most successful remote gaming operators.