MONEY LAUNDERING RISKS AND E-GAMING: A EUROPEAN OVERVIEW AND ASSESSMENT

Final Report

© Michael Levi, Ph.D., D.Sc. (Econ.)

Professor of Criminology

Cardiff School of Social Sciences

Cardiff University

Wales, UK

September 2009

CONTENTS

ACKNOWLEDGEMENTS

I am grateful to the European Gaming and Betting Association, especially Florian Cartoux, for their support for this project; to the compliance officers, payment card experts, police, professional gamblers, regulators and UK Payments staff who gave of their expertise and time, and commented on earlier drafts; and to Michael Gold for his research assistance.

Michael Levi is currently funded by a UK Economic and Social Research Council Professorial Fellowship (RES-051-27–0208).

EXECUTIVE SUMMARY

This report reviews the threat that money laundering through the e-gaming industry presents and could plausibly present to society, and the ways in which the regulated e-gaming industry discharges its duty to reduce money laundering in the EU. Industry representatives interviewed agree that there can be 'leakage' through which launderers may move some proceeds of some crimes, **though the risks associated with the sector are comparatively modest, due to the high traceability of e-gaming transactions and the customer identification controls in the regulated sector**. However this report suggests that it is not a realistic policy goal for governments in a free society to eliminate money laundering risks altogether: the aim should be to reduce to a tolerable level the risk that e-gaming may assist other crimes. This is done in two ways: controls over ownership; and controls over the operation of e-gaming itself. One reason to prefer regulation over prohibition is to ensure that operators have to undergo a 'fit and proper person' test before receiving a licence, preventing people with links to organised crime and terrorist groups from owning what could be vehicles for laundering if there were no controls or if controls were over-ridden by powerful managers or beneficial owners.[1] The second reason is to encourage e-gaming companies to develop a set of procedures approved by regulators to reduce integrity risks.

One question raised in this review is how plausible it is that a significant amount of this total laundering – in the billions of Euros - would occur via e-gaming. E-gaming (as contrasted with land-based forms of gambling) does not directly feature significantly, or indeed at all, in the recent published threat assessments of Europol and other European policing organisations, or in their policing priorities. To date, generalised and understandable expressions of concerns by Europol and by the Financial Action Task Force about money laundering risks posed by the Internet have *not* been accompanied by evidence of significant laundering via e-gaming.

AREAS OF RISK

1. Online gaming firms can credit winnings or unused funds back to an account other than the one on which the original bet was made: an issue which gaming firms share with other business areas**.**

2. The use of 'front people' through whom to run gaming transactions.

3. Peer to peer games, where value transfers can occur between both electronic and human players as a result of deliberate losses, at a relatively low cost to the players.

4. Payment in (and out) via other financial intermediaries which are regulated for AML purposes but where Know Your Customer is of modest or variable quality.

The corrupt 'fixing' of sports results or individual events on which betting takes place, generating fraud and proceeds of crime, is sometimes considered to be money laundering. However this is the making of a dishonest profit rather than hiding and transforming the proceeds of crimes that have been committed in the community. Likewise, identity fraudsters can use financial instruments they have acquired to gamble for pleasure and to transfer modest sums to other media: but this is more fraud than it is money laundering.

[1] A 'beneficial owner' is someone on whose behalf a company is run, whether or not they are listed on documents as the nominal owner.

EFFORTS TO COMBAT MONEY-LAUNDERING

Online gaming companies licensed and regulated in the EU have chosen to comply with the Third EU Directive for the prevention of money-laundering which – strictly speaking – applies only to casinos within the gaming sector. In addition, the regulated sector also subscribes to codes of conduct such as that of the European Gaming and Betting Association[2] and the Remote Gambling Association.[3]

On-line gaming companies collect a significant amount of data on the IP addresses, gaming and gaming finance patterns of their customers, which are used to build up profiles against which to assess the risks posed by particular customers. E-gaming firms vary in the extent to which they impose spending limits, and in general business sectors and financial services, this would be regarded as a purely business decision, unless their solvency was threatened, which in this case would be very unlikely. Greater diligence is (and should be) exercised where gaming limits are higher, since this generates greater laundering opportunities.

All the businesses interviewed have different business models, and consequently implement risk based solutions to mitigate the potential for anti-money laundering and crime risks. The operators interviewed acknowledge that there is no single magic bullet to combat crime, but that a cocktail of tools – which may vary over time - is required to combat any risks in a proportionate manner. Consequently they employ a hybrid anti-fraud model using a combination of techniques including but not limited to manual, external data checks, internal business rules, statistical profiling. In addition, some businesses are utilising are or intend to utilise advanced machine learning techniques. Analytically, these may be split up into categories as follows:

- *Manual*
  - Agents flag cases they consider to be "suspicious" based on risk alerts, customer tip-offs and unusual betting and or wagering play by customers

- *Third Party Data*
  - Age Verification lists sourced from firms in the market
  - Hotlists, including the sorts of data sources used by banks to identify terrorists and public officials (entitled 'Politically Exposed Persons') who require 'Enhanced Due Diligence'
  - Telematching
  - The European Sports Security Association watch list

- *Rules Based*
  - Pre-defined rules based on business knowledge and past experiences. For example limitation on the number of credit cards that can be used; device reputation models

- *Statistical Profiling*
  - Outliers of transactional behaviour determined through regression analysis
  - Risk scoring models

- *Advanced Analytics – Artificial Intelligence*
  - Creating predictive modelling techniques
  - Implementation of neural networks to assist the human thought process in detecting fraudulent trends

[2] http://www.egba.eu/pdf/EGBA_Standards_March_2009_EN.pdf
[3] http://www.rga.eu.com/shopping/images/RGA%20SR%20Code%20-%20%20Final%2007.pdf

Compared to methods of customer identification and monitoring in the off-line gaming and financial services sector, the scope for substantial abuse of e-gaming for laundering purposes is modest, both for those crimes that generate cash and for those that do not. This is partly a result of the greater recording of transactions in this industry than in most others, and partly the consequence of legitimate firms being subject to regulation.

The industry does make efforts to identify and report suspicious activities by customers, though – as in every area of commerce – firms have different approaches to this. In itself, the number of Suspicious Activity Reports is neither a success nor a failure indicator of AML effectiveness. The more effective that front-line Know Your Customer (KYC) controls are and the less inherently exploitable an industry is to large post account-opening expansion of trading (enabling more funds to be laundered), the smaller the overall laundering problem that it poses: subject to their skills and contacts, offenders typically will search for easier ways to launder. Thus if money laundering controls are tight and are perceived by offenders to be tight - or if e-gaming is not contemplated at all by them as a laundering route - one might expect few Suspicious Activity Reports (SARs) to be made.

In the UK in 2007-2008, out of a total of 210,052 SARs, the gaming sector made 403 SARs (up from 299 in 2006-07), of which 24 involved requests for consent to permit dealing with a person whose transactions they suspected of being proceeds of crime: however there is no breakdown for e-gaming compared with land-based gaming. By way of comparison, there were 33 reports direct from credit card companies,[4] and 280 reports from spread betting firms; 7,299 reports from money transmission firms, and 3,553 from bureaux de change.[5] One SAR from the gaming sector was considered sufficiently indicative to be transmitted to the National Terrorist Finance Unit for further investigation. Analogous data are not available EU-wide.

CONCLUSIONS

Risk levels are a combination of criminal motivations, existing/developing criminal capacities, and situational opportunities for crimes offered by the ways control is organised. There is scope for improvement in controls over fraud and laundering, and regulators need to be vigilant about the levels of resourcing of anti-fraud/AML efforts in the private sector and internationally consistent in their requirements, following deliberation between different regulators and consultation with the industry. There is much mythology about e-gaming laundering risks, fed by inadequate information and a tendency to project a dislike of gaming and/or private sector involvement in it into alarm about e-crime in general and the role of gaming in this. While taking account of businesses that offer both land-based and internet gaming, it is desirable to have separate AML regulations for *e*-gaming, since opportunities for monitoring are so different. E-gaming using those Stored Value Cards (and, in the future, media such as payment-enabled mobile phones) that have *not* been through adequate KYC controls requires special attention. Not all laundering via e-gaming can be eliminated, but because of the controls over the number of cards used per account-holder and the electronic monitoring of location and IP addresses, there is no evidence that the *general* risks posed by e-gaming are serious compared with other methods of laundering the proceeds of crimes.

[4] Credit card issuers in the UK obtained exemption from the requirement to submit SARs after every fraud, because to do so would place an unreasonable administrative burden both on them and on the Serious Organised Crime Agency (the UK's Financial Intelligence Unit) for no obvious enforcement/intelligence benefit since, in most cases, there is no suspect.

[5] See the Serious and Organised Crime Agency (2008: 41).

1. INTRODUCTION

This is a review of e-gaming and the money laundering risks that can and are known to arise from it, from the perspective of the EU. It may be helpful first to outline what money laundering is, and it will be argued here that there are two significantly different ways in which people use the term 'money laundering'. The first is to mean the hiding of the illicit origins of funds in order to make tainted wealth look legitimate. This, we suspect, is what most people who encounter the term would expect money-laundering to mean. The second – acquiring, possessing or using proceeds of crime - comprises all acts that fall within the laws and regulations against money laundering, which are intentionally framed broadly in order to stimulate business, finance and the professions to make it harder for criminals to legitimate their wealth in the first sense above. It also penalises broadly defined self-laundering by those who commit the primary money-generating crimes (often referred to as 'predicate crimes'), to the extent that almost anything they do with proceeds constitutes laundering. The preventative role in avoiding damage to the integrity of the single European market is the reason why the European Community first (in 2001) regulated laundering under the First Pillar of the EU rather than the Justice and Home Affairs Third Pillar.[6]

WHAT IS MONEY-LAUNDERING?

Article 1 of the Third Money Laundering Directive of the European Union (2005/60/EC) requires the prohibition (in law) of money-laundering and terrorist financing in the following terms:

> "2. For the purposes of this Directive, the following conduct, when committed intentionally, shall be regarded as money laundering:
>
> > (a) the conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of his action;
> >
> > (b) the concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to, or ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity;
> >
> > (c) the acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity;
> >
> > (d) participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counseling the commission of any of the actions mentioned in the foregoing points.
>
> 3. Money laundering shall be regarded as such even where the activities which generated the property to be laundered were carried out in the territory of another Member State or in that of a third country.
>
> 4. For the purposes of this Directive, "terrorist financing" means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out any of the offences within the meaning

[6] The extent to which money laundering does have this destructive effect on financial institutions lies outside the parameters of this study.

of Articles 1 to 4 of Council Framework Decision 2002/475/JHA of 13 June 2002 on combating terrorism [9].

5. Knowledge, intent or purpose required as an element of the activities mentioned in paragraphs 2 and 4 may be inferred from objective factual circumstances."

This is a very broad prohibition of any acts that are knowingly performed with the proceeds of crime (and, in the case of terrorist financing, acts with legitimate funds that further terrorism). It also appears to encompass leisure expenditures that derive from the proceeds of crime, as well as laundering in the sense of concealing proceeds in order to reinvest with the appearance of legitimacy.

2. Risks and Threats in Money-laundering and e-Gaming

There has been a slow evolution in the understanding of money-laundering and responses to risk. In the first phase during and after the international criminalisation recommendations in the 1998 Vienna Convention, analysts examined what they took to be the most common forms of money-laundering in the cases of which they had knowledge: mostly proceeds of cash-generating crimes. In the second phase, accompanying the growth of the range of predicate offences and of the number of areas of commerce regulated by AML (from the initial focus exclusively on financial services businesses), some conceptual work was done to identify the ways in which criminals might be able to launder moneys, though there was little effort to examine how commonly these vulnerabilities were actually exploited or, indeed, what the impact of such exploitation might be on society or on levels of different crimes.[7] In the current welcome phase of risk-based approaches to financial crimes, a greater level of thought is being given to the prioritisation of public and private sector resources and to benefit-cost analysis of different sorts of interventions into areas of social harm, though there is less *fiscal* pressure on governments to do this in money-laundering than in many areas of crime control, because many of the costs of identifying customers and of suspicious behaviour are borne initially by the private sector and then ultimately by consumers. There is also less *political* pressure to refrain from extending regulation because, in the image and substance of corporate social responsibility, respectable businesses and professions do not want to be seen as 'assisting crime'.

The aim of this review is to contribute to this more developed thinking in one particular area of money-laundering risk: that related to e-gaming or remote gambling.[8] This includes the following areas of activity (s.4, UK Gambling Act 2005):

- Remote Wagering on Horse Races
- Remote Lottery Play
- Online Telephone Race and Sports Books
- Multi-Player Online Poker through interactive poker rooms

[7] The level of current exploitation is not definitive here, since it is an indication of past activity, not future threats: it is quite reasonable to examine vulnerability independent of actual misuse, provided one does not represent that as a fully developed risk analysis.

[8] Gaming is defined in the Oxford English Dictionary on-line as "The action or habit of playing at games of chance for stakes; gambling". Gaming is often understood as legal gambling: to gamble is defined as "To play games of chance for money, *esp.* for unduly high stakes; to stake money (*esp.* to an extravagant amount) on some fortuitous event. As the word is (at least in serious use) essentially a term of reproach, it would not ordinarily be applied to the action of playing for stakes of trifling amount, except by those who condemn playing for money altogether."

- Online Casinos offering online gambling through games such as blackjack
- Betting Exchanges – peer-to-peer betting exchanges by which individual bettors can place wagers against one another on opposing outcomes of a future event
- Interactive Gambling - including traditional betting wagering forms as diverse as traditional betting to fixed odds gambling, live and interactive bingo betting and interactive betting on live sporting events.

It will be argued that e-gaming *does* present money-laundering risks, but that - despite the evocations of alarm and evil (see Bauer, 2008) that often accompany the 'e' word attached to crime (Levi, 2008, 2009) – in a *regulated* environment, the risks are lower than in land-based gaming and in cash-based businesses, due to the high traceability of transactions, betting limits and customer identification controls in the regulated sector. If e-gaming firms were unregulated, AML would be wholly dependent on controls exercised by card issuers and merchant acquirers. To combine the risks from the regulated and unregulated gaming sectors would be a fundamental mistake, just as it would also be a mistake to merge regulated and unregulated banking, accounting, etcetera, unless one could demonstrate that regulation makes no difference to risk.

There are very few areas of social and commercial life that present no crime risks.[9] Instead of seeing crime risks as binary (risk/no risk), contemporary threat assessments envisage threats in a more graduated linear way, in terms of both (i) vulnerability to exploitation, *and* (ii) the capacity of existing and future offenders *and the networks and 'organised crime groups' to which some of them belong* to exploit those opportunities and to do harm. However there remain problems of how we judge risks to individual countries or groups of them such as the EU: the Financial Action Task Force (FATF) is in the process of developing a global threat assessment for money-laundering, but though improving, the underlying empirical basis for such an assessment is currently weak, since systematic collection of knowledge even of behaviours in the public domain is at best intermittent. There are three sorts of criminal situations[10] in which businesses are involved that are relevant to threats against e-gaming firms and the public:

- perpetrators who use businesses as tools to victimise others (like fake gaming websites to collect card and other personal details which can then be used fraudulently, on-line or off-line);
- perpetrators who utilise businesses to facilitate other crimes (e.g. wholly or partly as money-laundering vehicles); and
- perpetrators who use their positions inside businesses to commit substantive crimes (from duplicating customer identity details to defrauding the companies for which they work).

The key points to be examined here is what money-laundering harms theoretically *could* follow from e-gaming; what do we know about how commonly these are *actually* exploited; how (if at all) would we know if these opportunities were exploited at a significantly greater rate than at present; and why would offenders (in general, or particular sorts) choose to launder funds through e-gaming rather than through other mechanisms.

There is much dispute about the total volume of proceeds from crime, and little evidence about how this varies between different sectors of the wholly illicit and partly illicit economy. The often-quoted IMF estimate is based upon very little evidence (Levi and Reuter, 2006), and mere repetition does not compensate for its lack of underlying validity. UK government economists have estimated a mid-point figure of £30 billion annually for trafficking in drugs and people, fraud and financial crime generated in the UK (Cabinet Office/Home Office, 2009), but even accepting this as a very rough order-of-magnitude figure, this tells us

[9] This is not to accept or reject more general arguments about the positive and negative consequences of e-gaming: it is rather that these are not germane to the present project on money laundering risks.
[10] These situations are not mutually exclusive.

nothing about what proportion of these proceeds is laundered (in the narrower sense of saved and/or re-invested in the licit economy). There are no equivalent defensible estimates for the EU as a whole, but the total sum would obviously be very large. One question raised in this review is how plausible it is that a significant amount of this total laundering would occur via e-gaming.

The financing of terrorism presents different issues: because direct operational costs[11] of the London and Madrid bombings are under €10,000, very small amounts of laundering may be critical to terrorists' success. But since terrorism can be funded by both licit and illicit activities, the range of behaviours that could generate such sums is so vast that it is almost unmonitorable without sophisticated aggregate models and/or listing individuals and institutions believed to constitute such a threat. Thus e-gaming is only one potential source of terrorist finance among many others; and even if it was connected with terrorist plots (as some newspaper sources have claimed and as is evidenced in one UK case), terrorists would not have found it difficult to find another source of funding or 'value transfers'.[12]

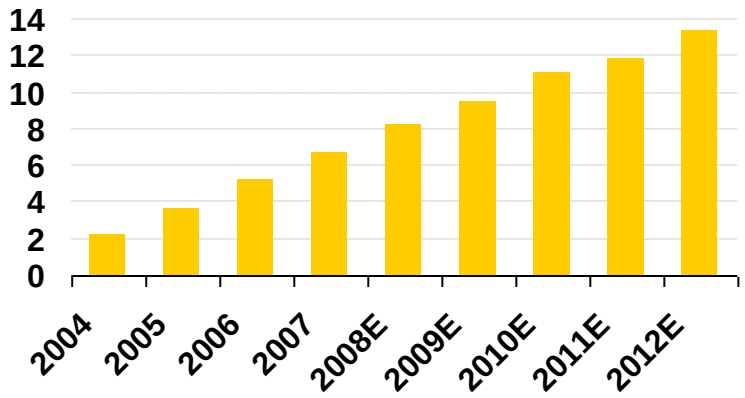
E-GAMING IN EUROPE: THE ECONOMIC CONTEXT

Let us look at the money laundering risks within the perspective of the size of the on-line betting and gaming industry. On-line gambling accounts for some 5% of global Gross Gaming Revenues (stakes minus winnings). European players constitute around half the global market for on-line gaming (excluding lotteries). In 2009, H2 Gambling Capital estimated Gross Gaming Revenues in the European gaming market at €85 billion for 2008, of which €6.5 billion (7.65% of the total) was in online gaming. Three quarters of this (€4.8 billion) went to private operators, the rest going to state monopolies. On-line gambling volumes are projected to rise significantly by 2012, but the public/private sector ratios are not expected to change. Global Betting and Gaming Consultants (2008) have produced past and projected estimates of gross gaming revenues for the European market, in US$ billion, set out overleaf. It is within this economic context of very substantial expenditures that money-laundering risks should be viewed.

[11] This excludes the broader costs of creating a climate in which support for terrorist acts is stimulated, and of the indoctrination, recruitment, and preparation of potential attackers.

[12] As the report by MHA (2009: 32) notes, the only publicly identified case is that of Tsouli and Al-Daour in July 2007. To elaborate on their account, the defendants had together purchased web sites using stolen identities and credit card details on which were then published the extreme propaganda and recruiting material produced by al-Qaeda in Iraq. The material was crafted to incite and recruit suicide bombers accessing the websites and forums internationally, comprising as it did graphic and emotive media. It included daily statements and films of the murder of coalition forces, police, officials and civilians, together with footage of the beheading of hostages (http://www.cps.gov.uk/publications/prosecution/ctd.html#_10). Al-Daour allegedly laundered money through online gambling sites, using accounts set up with stolen credit card numbers (http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/03_06_08_fo4_terror.pdf). He and other members of the group conducted 350 transactions at 43 different online gambling sites, using more than 130 compromised credit card accounts. Winnings were withdrawn and transferred to online bank accounts that the men controlled, with the help of insiders. The media portrayed the case as the world's first cyber-terrorism trial. The media did *not* report that a number of attempts to launder through a remote gambling site were unsuccessful (and incompetent) and were identified, Suspicious Activity Reports were submitted to the authorities, and the accounts were closed. Thus, the AML system did its work as well as it could and as it is hoped that it will in the future.

GROSS GAMING REVENUES (BILLION EUROS) FOR THE EUROPEAN MARKET



Gambling (a wider category than just e-gaming) accounts for 2.2% (by volume) and 1.2% by value of total plastic card spending at UK acquired merchants. According to UK Payments, the trends for plastic spending on gaming in the UK are as follows:

	Volume (000s)	Value (m)	Average Transaction Value
2004	65,234	£1,975	£30.29
2005	86,945	£2,641	£30.38
2006	113,193	£3,312	£29.26
2007	128,117	£3,511	£27.40
2008	130,155	£3,562	£27.36

MONEY-LAUNDERING TECHNIQUES

The modern construction of money laundering sees the phenomenon as involving the transfer of value from one medium and/or geographic place to another. The depth of concealment involved in this process depends on:

1. The form in which the crime proceeds are obtained (e.g. cash, electronic payments, merchandise)
2. The skills and contacts of potential offenders
3. The skills and contacts of intermediaries acting on behalf of offenders
4. The 'capable guardianship' capacities and motivation of those private and public sector organisations that may be required in order to carry out the laundering activities, and
5. The legislation, resources and skills of those investigating the offences and offenders.

Any given offender or set of offenders (e.g. the rather loosely defined 'organised crime group'[13]) may have different requirements. Most low-earning offenders have no need to launder, because they spend fairly soon

[13] According to Europol and the UN Transnational Organised Crime Convention 2000, this is three or more offenders acting together over an undefined period to commit crimes for gain: not a very difficult threshold to meet. The Europol (2008) Organised Crime Threat Assessment states (p.16) that "EU-based groups refer to OC groups that have both their leaders and at least a substantial part of their assets inside the EU". There has been a shift in the Europol mandate from 'organised crime' to 'serious crime' which avoids the definitional problems surrounding organised crime: but since the latter term is

what they make from crime: part of that expenditure may be on e-gaming but except in the most trivial of senses, this does not constitute laundering in its common meaning of concealment and legitimation of savings from crime. Gambling is no different in practice from spending the funds on alcohol, cigarettes, foreign holidays, or any other means of consumption using up proceeds of crime: by this criterion, not just on-line and off-line betting and gaming firms (*private and public sector*), but also airlines, bars, holiday firms, restaurants who service criminals might all be suspected money-launderers. Laundering for savings and reinvestment – as in the classic tripartite placement, layering and integration model that has been used in the FATF since 1998 - only occurs when people either (i) are living disciplined lives and building up (at least partly) licit businesses for the future or (ii) have generated so much proceeds that part of those proceeds becomes what economists term 'forced saving'. The point at which the latter occurs is related to their lifestyle expenses, which can shift over time: a phenomenon not restricted to *illicit* income.

LITERATURE REVIEW OF MONEY LAUNDERING IN E-GAMING

E-gaming (as contrasted with other land-based forms of gambling) does not directly feature significantly, or indeed at all, in the recent published threat assessments of Europol[14] and other European policing organisations, or in the policing priorities that accompany or develop out of them. This is confirmed in the informal discussions that this author has had with appropriate persons who work for them. The expression of concerns about possible risks of the Internet does not evidence laundering via e-gaming.[15] In addition to Europol, the Netherlands and the UK (and, outside Europe, *inter alia* the Financial Action Task Force, Canada and the US), a small number of private sector bodies are also producing 'threat assessments' based around their analyses of the harm from particular areas of criminality such as fraud (CIFAS) and intellectual property crimes (FACT). These sidestep some of the definitional problems accompanying the 'organised crime' terminology, but they too try to separate risks arising from opportunists and those from career criminals. It is not as difficult for industry bodies to examine the risks to their members from predicate crimes of which they are the victims as it is to measure the risk from laundering proceeds of those crimes of which they are not victims themselves.

---

still being used within the European arena, better clarification of what is and is not 'organised crime' and what it takes to become defined as an 'OC group' would make evaluating the adequacy of responses to threats from it more meaningful.

[14] An older Europol (2005) report, compiled under the now outdated model rather than the post-2006 Organised Crime Threat Assessment (OCTA), stated (p.17) "In some Member States legal gambling schemes are quite a widespread modus operandi to launder money. It is estimated that the above-mentioned trend will continue and increase in the future. OC groups also make their way directly into the gambling world by buying companies in this field." The owners and directors of regulated gaming firms are required to pass 'fit and proper person' tests, so depending on the quality of regulation, we may assume that the older Europol comments are irrelevant to this study and that the allegation is of a highly general nature. Some later threat assessments and situation reports mention risks from gambling, but not e-gaming.

[15] Among the sources that provide no evidence to suggest that e-gaming is a significant source of money laundering risk are:

- United States General Accounting Office, *Internet Gambling – An overview of the issues*, 2002, p. 34 et seq http://www.gao.gov/new.items/d0389.pdf
- The 2007 report of the German Financial Intelligence Unit at the Bundeskriminalamt http://www.bka.de/profil/zentralstellen/geldwaesche/pdf/fiu_germany_annual_report_2007.pdf, the relevant section of which repeats the wording from the Europol report of 2005.
- The report for the French Parliament by Blessig and Myard (2008: 89-90) - http://www.assemblee-nationale.fr/13/pdf/europe/rap-info/i0693.pdf;
- The French Lexsi report, *Cybercriminalité des Jeux en Ligne*, www.lexsi.com/telecharger/gambling_cybercrime_2006.pdf

Historically, e-gaming risks have often been placed in the same category as two other areas of commerce: (i) gaming/ gambling generally[16] and (ii) e-gold and other forms of e-wallet/pre-paid cards that are designed to transfer funds. It is important to understand the basis for some of the risk statements made, and how these can vary over time and place, a variation not always appreciated in some critiques of on-line gaming risks (Bauer, 2008). There is an enormous difference between the limitations imposed on pre-paid cards in a European and in American context, Europe placing low limits on payments into pre-paid cards and imposing some customer identification onto them, while the pre-paid cards that generated FATF concern had high limits and no significant customer identification or post-purchase monitoring. (For a discussion of risks arising from Stored Value Cards, see Choo, 2008). To date, there have been no AML regulations designed with a specific focus on *e*-gaming. Thus the thoughtful FATF risk-based review of casinos (2008a) treated Internet casinos as a special case of casino, noting the lower risks normally attached to the former than the latter (see Annex A at the end of this review). The FATF (2008b) report on internet payments noted (para 4):

> The financial transactions that are initiated from a bank account or a credit card (which is the majority of online payments) already involve a customer identification process as well as transaction record keeping and reporting obligations. While low value transactions do not necessarily equate to low risk, these transactions are subject to the regulatory controls already applicable to the financial sector and may be consequently less risky. Regarding the risks associated with the non-face-to-face registration and the possible anonymity of the users, the study highlights the need for online identity verification solutions (the electronic identity card used in certain countries for instance) to help commercial websites and Internet payment service providers mitigate the risk of criminal activity….If Internet payment service providers adequately monitor the financial transactions of their customers, monitoring for and acting on deviations from the customer transaction profile, the lack of face-to-face contact at the beginning of the relationship with the commercial website and Internet payment service provider may not constitute a problem. Online and offline retail merchants and payment services should have comparable AML/CFT obligations.

However it is important to disentangle the levels of risk from different products. One important distinction arises out of the legality or illegality of e-gaming itself. Where, as currently in the US and some European countries, e-gaming offered by private operators is *per se* illegal, the knowing use of such funds by e-gaming firms arguably[17] becomes money-laundering because under the 'all crimes' laundering model mandated by FATF, e-gaming is a predicate act and all concealment, disposal and assisting in the disposal of funds etc. obtained from e-gamers becomes money-laundering. Thus in the US and in some EU countries, e-gaming offered by private operators presents a serious problem of money-laundering because (*and only because*) e-gaming is criminal and because many people like to bet, both on-line and off-line. By contrast, the identical behaviour engaged in within the UK presents very little money-laundering risk because the gambling is not a predicate crime. So from an overall EU perspective, it is problematic to include within a crime threat framework activities such as e-gaming itself that are legal in parts of Europe.[18] What is more significant and

[16] There are signs of a more sophisticated and nuanced approach emerging. The FATF/APG Report on Vulnerabilities of Casinos and Gaming Sector notes (2009: 56):

> "197. While this study has not included online gaming/online casinos in its scope of enquiry, it is clear that there are a number of related risks and vulnerabilities from online casinos. A number of jurisdictions license physical casinos and online casinos under a similar process. This report notes a significant gap with understanding regional money laundering risks and vulnerabilities from online casinos and online gaming. There is a need for further study in this area and for sharing case studies and regulatory models."

[17] There is a difference between the US and the EU, not just because of differences in the AML regime, but because there is a genuine dispute over the constitutionality of prohibitions against a free market in private sector e-gaming within the Single European Market.

[18] Of course, it could be argued that just as all crimes are artefacts of the criminal law, by definition, *all* money-laundering risks are an artefact of criminalisation of their predicates. However we mean something more than this truism here. The distinction we are making is between acts that are universally regarded as harmful and acts such as e-gaming where this is

worthwhile is to examine the use of e-gaming to launder the proceeds of crimes other than (where the gaming is prohibited by criminal law) the activity of e-gaming itself. Financial institutions have primary responsibility for Know Your Customer (KYC) on their account-holders. As the FATF (2008a, b) concedes, the fact that e-gaming requires funds from a financial institution suggests that these risks are not high (or, one might add, are at worst no higher than any activity perpetrated via an account with a licit savings institution).

AREAS OF MONEY-LAUNDERING RISK

Risks from (and to) offenders are also a function of controls, discussed further in Section 3 of this report. One area of risk relates to the possibility that e-gaming firms can credit winnings or unused funds back to an account other than the one on which the original bet was made: an issue which gaming firms share with other business areas**.** Payment card firms normally do not allow winnings and cash-ins to be credited to card accounts other than those used in the original gaming transactions,[19] though they may be obliged to do so if the customer insists (while having the option to report this as a suspicious activity to the appropriate Financial Intelligence Unit). They may also pay the customer by cheque or other means of payment, even if the original payment in was made by card. To the extent that they do, and especially if they reimburse to cards in names other than that of the original gamer, this is a control weakness in relation to the risks of both card fraud (the original card may have been stolen or the card/card data counterfeited) and more general laundering of the proceeds of other crimes. If detected after the fact, e-gaming on stolen cards/card numbers imposes charge-back costs on gaming firms – which escalate once the charge backs reach a percentage of turnover (Visa) or number of transactions (MasterCard) - and it also imposes (mainly) non-economic costs on cardholders (who – as in all fraud and overcharging cases - have to go to the trouble of complaining and getting the costs reversed). The funds credited to the other account will be proceeds of crime, and therefore money laundering even where the card-holder does not lose financially.

However for the assessment of the *general* risks posed by e-gaming, what is crucial here is the *scale* of the repayments to other cards or forms of funds that is allowed, and the time over which this is possible without controls kicking in: for card fraudsters, such 'windows of opportunity' are fairly crucial, since elapsed time enhances the risk of reporting and discovery. (Though even if discovered, the actual and perceived risk to offenders of criminal action being taken against payment card fraudsters is modest because of criminal justice resource constraints and priorities in many EU MS.) Offenders would have to work quite hard to move significant quantities of funds via e-gaming, and it is not obvious why they would bother with this process at all if they were *not* generating large sums from crime. The fact that losses from charge-backs (for rejected card transactions made on counterfeit or stolen cards/card numbers) are less than 1 per cent of total funds deposited – below the industry average - suggests that the level of card fraud used for e-gaming is under control and that this component of the risk is not severe, though the total Euro value of sums charged back (and therefore obtained/transmitted by criminals) may be large. Charge-backs may not reflect laundering (moving funds to obscure the illegality of the source) as much as the gambling appetite of risk-taking criminals, enjoying gaming at what is in the end the expense of the gaming firms themselves, since cardholders and merchant acquirers are reimbursed for their losses. Some of the gaming is stopped by the e-gaming firms themselves because it does not correspond to the risk profile of cardholders. Far more data are available for e-gaming firms to develop such profiles than in almost all off-line environments.

---

substantial disagreement both about how harmful the behaviour is and whether those harms should be dealt with by the criminal law or by the more subtle controls that accompany money-laundering regulation. Overall net benefits/dis-benefits of e-gaming are out of scope for this review.

[19] Payment into what is termed 'non-originator' cards is forbidden by the scheme rules of Visa and MasterCard, while American Express does not permit expenditure on internet gaming. In Australia, it is legal to use credit cards for e-gaming, but it is not permitted to credit winnings to such cards, the object presumably being to make gamblers think harder about playing. There, they cash in winnings by bank transfer, cheque or other mechanisms.

A second area of risk arises from the possibility of using 'front people' – i.e. nominees acting for undisclosed principals - through whom to run gaming transactions. This can be done in any area of financial services also, as in the case of students being paid as 'mules'[20] to allow their personal accounts to be used as conduits for transfers from overseas. At a more serious level, launderers can pay businesspeople (or covertly act as beneficial owners themselves) to merge proceeds of crime with their normal takings: this is a risk that is heightened at times of economic pressure. They can also purchase lottery and other winning bets from the real winners (at what marginal laundering cost mark-up is unknown) so that they get a cheque/electronic payment from a legitimate-source agency that should disarm bankers' suspicions of money laundering: however there is a limit to how many such wins – especially lottery wins – anyone can plausibly get to defeat suspicions by bankers and/or of any criminal investigators if they do not accept these explanations of wealth at face value. So although people prohibited from gaming in their own names (because they are too successful and lose gaming firms money) can use front people to conduct their gaming covertly, one might question why *launderers* of crime proceeds would do so when there are so many other avenues for concealment of beneficial ownership.

A third area of risk arises in the context of peer to peer games, where value transfers can occur between players as a result of deliberate losses. Such losses do not generate any direct financial risks for the e-gaming firms themselves, and therefore their only motive for intervention is the avoidance of reputational or regulatory/penal damage.[21] However in addition to widely available poker manuals on probabilities of winning for different hands that generate 'expected data', they have expert players observing such games, whose judgment that players are losing deliberately can lead to the freezing of transactions and accounts, and perhaps to suspicious activity reports (SARs). No data are available on the extent to which such gaming account/transaction-freezings or SARs are actually made under these circumstances, nor is it known (or arguably *knowable*) how many potential launderers are deterred by their expectations of industry surveillance and intervention: therefore there are no reliable estimates of how effective such measures are in practice. One professional gambling arbitrageur expressed the view that, though some major firms were highly vigilant in fraud and AML prevention, it was possible to use programmed matched electronic 'bots' to offer and accept poorly judged odds, using as distracting screens the fact that many such 'bots' do take partial stakes in bets and sometimes through 'software bugs' make foolish gambling offers. So long as the players stayed within the range of acceptable error and behaved as bots might be expected to behave, they could relatively cheaply (in commissions to gaming firms) transfer sums that might be significant to some 'offenders' such as 'tax dodgers', but that were far smaller than major crime syndicates would need to launder. However, it is not possible to judge the extent to which this possibility is a significant actual realised risk and threat to society (rather than to the betting and gaming industry, which is not impacted negatively directly by such activities).

A fourth area of risk arises from the possibility of paying via other financial intermediaries which are regulated for AML purposes but where KYC is of modest or variable quality (as in the mainstream financial sector also). In addition to credit cards,[22] such payment media include bank transfers, debit cards, Cactus,[23] Moneybookers,[24]

[20] So called because they are allowing themselves to serve as transporters of other people's property.

[21] If there are parties other than the conspirators playing the game, they may become annoyed if they think that one party is cheating, and therefore cease playing with the site on which the suspected cheating occurs. This would constitute an economic opportunity cost for the gaming site.

[22] These are variable, depending on the firm. However for at least one regulated operator, minimum limits which apply to deposits are EUR 10 and the minimum limits which apply to withdrawals are EUR 30. Daily maximum limit per credit card: EUR 1000. Monthly limit per credit card: EUR 5000.

[23] Cactus is a prepaid MasterCard® and eAccount. Unlike a credit card, customers can only spend the money they have pre-loaded; unlike a debit card, the Cactus Card is not linked to a bank account so fraudsters could not get to the bank account through it.

[24] Moneybookers – which is regulated by the Financial Services Authority - allows customers to send and receive money via e-mail. Moneybookers' wallet allows them to make safe deposits and out-payments instantly; it requires identity verification before using their service to minimize fraud and prevent money laundering.

Neteller,[25] PayPal, Paysafecard,[26] and Ukash.[27] One of the drivers for increased take-up of such standalone payment media not linked to people's bank accounts is fear of fraud from data theft: however this report has not had sight of any market research showing the extent to which that is the case. Funds used to purchase e-money can come from legal sources, licit but tax-evading sources, or wholly criminal sources. It is obviously possible for criminals to use the proceeds of crime to purchase e-wallets or vouchers that can be spent on e-gaming and on more tangible commodities. Persons using these more anonymous media are still, however, subject to the customer identification and trading pattern checks of the e-gaming firms themselves, which include bans on multiple identities playing from the same geo-location/IP address. Thus even the leisure expenditure by criminals on e-gaming would be subject to controls if they are using fraudulent cards.

The final area of risk to be mentioned here is different from the others, but arises from the FATF (2009) review of *Money-Laundering Through the Football Sector*. The report states that separate attention should be paid to laundering via legal and illegal betting but (p.8, para 26) this is a 'huge and increasing problem', though the empirical grounds for this view remain obscure. It adds (p.24, 25):

> **Betting activities**
>
> 79. There is an ambiguous relationship between betting and sport. On the one hand, betting has historically been an important revenue source for sport in many countries. On the other hand, betting has also been associated with attempts to fix matches and alter the results of sporting competitions. Betting can be used both for the generation of illegal proceeds from game fixing and for pure money laundering purposes.
>
> 80. The FIFA Task Force "for the Good of the Game" has observed that "due to its particular structure, as well as the considerable need to finance the system at short notice, football offers a tempting platform for irregular betting activities. As the media and the public eye focus on fixtures in top competitions and top leagues, irregular betting activities can frequently be observed in less important fixtures (including lower divisions of domestic championships), where the environment can be manipulated more easily. Recent scandals in which betting has resulted in the manipulation of matches have brought the game into serious disrepute".
>
> 81. While problems linked to betting are not new, it appears that betting in sport has reached new levels of sophistication with various operators involved across several countries and continents and new offshore betting companies being established. Moreover, the use of the Internet for online betting further increases the risk of money laundering.

[25] NETeller – which is regulated by the Financial Services Authority - is a specialist in internet funds transfer. After undergoing customer identification, NETeller customers are required to open a virtual bank account, where they may either deposit or withdraw funds at their convenience. Transactions deposited into or withdrawn from this account are executed within the same day. (Limits when depositing at one e-gaming firm: Minimum daily limit: US$ 30. Maximum daily limit: US$ 1.000. Maximum monthly limit: US$ 5.000.)

[26] There are 20,000 local shops in the UK and over 230,000 outlets in 16 countries across Europe where paysafecard vouchers can be purchased. The customer pays for a voucher in cash and enters a 16-digit PIN code. S/he can combine up to ten paysafecards for a single payment, thus enabling them to pay sums up to a maximum of GBP 1000.

[27] Ukash's parent company is Smart Voucher Ltd., which is authorised and regulated by the Financial Services Authority in the United Kingdom as an electronic money institution. Users do not need a card, bank account, to be a certain age or to register. They do not have to give any financial details and their purchases remain anonymous. Ukash is easily available from many local shops, via Vodafone mobile and will shortly be available online. Ukash is regulated by the UK Financial Services Authority, Customers getting Ukash from PayPoint stores in the UK may be asked to prove they are over 18: if not proven, the voucher issued will not be redeemable at age restricted (18+) merchant websites. The website requests customers to let them know "of any web site accepting Ukash that doesn't undertake these checks effectively, even though they are legally asked to do so. Please email us or call on: 0808 234 6244". However under-age customers are unlikely to do so, if they wish to use Ukash to gamble with! Ukash vouchers are transferrable, but only if they are given the 19-digit PIN and value. Customers can spend as many vouchers as they like, but each transaction is limited to a maximum value of £500 or €750.

> 84. Due to the fact that most countries have different gambling regulations, the gambling market is non-transparent and is a heterogeneous market with a mix of private and state companies acting both nationally and internationally. Providers are often established in countries which allow the organisation of gambling activities or in countries that do not regulate or supervise gambling. It is however not easy to take legal action against providers who offer their services online and are established abroad. This in combination with the non-transparency of the gambling market makes betting an interesting money laundering vehicle for criminals.

This mixes up legal and illegal betting in a way that is unhelpful for the purposes of assessing risks in this report. Moreover, it does not separate out cases where the operating companies (and sometimes the clubs or horse owners, and other bettors) are the victims – as in corrupt fixing of overall or spread-betting results in order to ensure success – from those in which operating companies do not have a particular interest or risk of loss. 'The Internet' does indeed change the nature of most forms of social risk, but though the criminal courts may have difficulty dealing with data-driven cases, the large amount of data available in the *regulated* e-gaming sector makes it difficult to comprehend the nature of the extra risks attributed to e-laundering through the football sector. In some respects, this report makes an argument for the regulation rather than prohibition of internet gambling, but it is not self-evident that state-owned e-gaming generates few (or no) risks compared with private sector e-gaming. Nor does the FATF report make it clear in an e-gaming context whether the extra laundering risks result from fraud and corruption in the *betting* process, or from the laundering of the proceeds of other crimes. It is clear that the purchase and management of football clubs (and inadequacies in the identification of beneficial owners thereof) offer opportunities for placement, layering and integration: however there is little risk analysis that helps for the purposes of *this* report.

Choo and Smith (2008: 50-51) discuss the variety of risks arising in on-line gaming, of which the most relevant to this study are:

- Creating special programs to gain unfair advantages by modifying game software and data, by exploiting bugs and design flaws and reverse engineering the gaming program. The perpetrators then have a better chance of winning in competitions and tournaments that award winners with prizes (e.g. unlocking new car components or car models). These acquired virtual assets can subsequently be traded or sold.

- Designing cloned websites with the aim of gaining login credentials of legitimate players and committing other crimes including identity theft.

They argue that the future will see the continued development of malicious code by organised cybercriminal groups targeting the online gaming community. However, these risks are aimed more at 'domestic' gaming, Second Life and its virtual currencies than at the sort of e-gaming conducted via the regulated e-gaming sector. It is also possible to programme electronic bots to offer bets at unusual times which are taken up by other bots (both on 2-player tables or on 6-player poker tables which are unlikely to be occupied at those times) who win. Done occasionally so that the easy bet is not taken on by another player not in the conspiracy or is not identified as a suspicious pattern of play by the gaming firm, this can be used to transfer value. However, as a large-scale laundering mechanism, it is unlikely to be successful.

Since there continues to be debate about the risks from prepaid cards, it should be noted that *reloadable* prepaid cards in the UK, from Member Banks of the Card schemes (i.e. open loop) require the same Know Your Customer (KYC) checks as is required for opening a UK Basic Bank Account without a credit facility. There do not appear to be different legal limits on *reloadable* prepaid cards: the card is seen as merely the access device to the customer's account. However:

- As there is no ongoing banking relationship, *non reloadable* pre paid cards (fixed value) e.g. gift cards, do not require KYC.

- The maximum value on a non reloadable card is circa USD $ 750 in Europe. These cards are issued anonymously (no personalisation) and therefore do not have ATM (cash) access. General controls on them are more modest but some of the same analytical techniques used to control e-gaming fraud and money-laundering risks (geo-location, etc., IP addresses, etc.) can be used here also.

The 2009 E-money Directive (EMD), when adopted by EU Member States, will with effect from April 2011 make significant changes across European Community regarding jurisdiction and access rights to who can offer e-money on a prepaid card.[28]

There has been a significant rise in Card-Not-Present (on-line) payment card fraud generally, largely reflecting the enhanced controls over off-line and card/cardholder present risks generated by the spread of Chip and PIN in the SEPA (Single European Payments Area). In the UK, for example, phone, internet and mail order fraud rose 13% to £328.4 million in 2008 (a rise of 350% since 2000). Looking at internet fraud alone, £181.7 million of card fraud took place over the internet in 2008, an increase of 2% since 2007. Internet fraud now accounts for 55% of card-not present losses – though down from 61% in 2007. The *proportionate* fall in Internet losses may be an indication that fraud is beginning to migrate away from the internet to other card-not-present channels, such as the telephone. The vast majority of this type of fraud involves the use of card details that have been fraudulently obtained through methods such as skimming, data hacking, or through unsolicited emails or telephone calls (APACS, 2009). No information is available on the extent of such card fraud usage in the e-gaming sector, but industry sources confirm that this sector does not account for a significant part of fraud losses.

[28] DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the taking up, pursuit and prudential supervision of the business of electronic money institutions amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/EC. PE-CO_S 3666/09, 16 July 2009. http://register.consilium.europa.eu/pdf/en/09/st03/st03666.en09.pdf

3. COUNTER-MEASURES AGAINST FRAUD AND MONEY-LAUNDERING IN THE REGULATED E-GAMING SECTOR

Implicit in the earlier discussion is the existence of counter-measures. It is not possible to estimate what the level of fraud and laundering via e-gaming would be in an unregulated 'state of nature': however regulation is important in reducing the collateral damage caused by e-gaming and other forms of commerce, including the prevention of gambling by under-age persons. Below are the sorts of measures taken by the regulated sector against fraud and money laundering. As noted earlier, neither this report nor industry representatives interviewed deny that there can be 'leakage' through which launderers may move some proceeds of some crimes. It would be absurd to claim a total shut-out of laundering from the e-gaming sector; nor is it a realistic policy goal for governments in a free society to eliminate money laundering risks. In respect of money laundering, the aim should be to reduce the risk that e-gaming may assist other crimes. This is done in two ways: controls over ownership and controls over the operation of e-gaming itself. One reason to prefer regulation over prohibition is to ensure that operators have to undergo a 'fit and proper person' test before receiving a licence, preventing people with links to organised crime and terrorist groups from owning what could be vehicles for laundering if there were no controls or if controls were over-ridden. The second reason is to encourage e-gaming companies to develop a set of procedures approved by regulators to reduce integrity risks. The latter are discussed in greater detail below.

MONEY LAUNDERING CONTROLS IN THE ONLINE GAMING INDUSTRY

Online gaming companies licensed in the EU have chosen to comply with the EU Directives for the prevention of money-laundering, the third of which – strictly speaking – applies only to casinos within the gaming sector. In addition, the regulated sector has developed an agreed set of standards (see footnote 2 and 3). Some of these measures (see EGBA standards, principle 3) in relation to anti money laundering include:

- Identifying their customers (including their age) and checking their information in detail
- Preventative and detective controls or technology shall be in place to ensure that the prospect of cheating through collusion (external exchange of information between different players) is prevented.
- For protection against identity theft, the Code notes:
- Confidential customer information submitted at any point in time shall be protected from unauthorised or unnecessary disclosure.
- Customer credit card numbers stored on the system shall be secured from unauthorised use.
- Making use of the watch lists containing known or suspected members of terrorist organisations, to try to ensure that they do not hold accounts
- Using established lists of Politically Exposed Persons to implement Enhanced Due Diligence, as required[29]
- Monitoring the gaming and in-payment/pay-out behaviour of customers
- Limiting deposits (to a variable extent, since some firms do not have limits but rather monitor carefully those few gamblers who make large on-line deposits, e.g. over €2,000)

[29] Though given that combating Grand Corruption in millions of Euros is the main driver here, it would be strange if PEPs were using e-gaming to launder funds rather than simply to enjoy gambling. If corrupt public officials and their families can defeat banking controls in the EEA and Switzerland, e-gaming firms face a big challenge!

- Prohibiting direct payments between customers
- Prohibiting cash payments directly (other than via regulated cash-card/voucher firms)
- Automatic blocking of payments from countries that are not the same as the registered home country of the customer
- After identifying an attempt to launder money, reporting the information to the Financial Intelligence Unit and – depending on the jurisdiction and 'tipping off' rules – blocking the account/ending the commercial relationship.

Furthermore, they include (to a variable extent):

1. Device Fingerprinting -- Taking a 'fingerprint' of a device like a laptop enables them to check whether it has already been used by an identified fraudster and/or launderer.
2. Location mismatches -- Running rules looking at a customer's physical location (and from where they are logging in) and their telephone number to look for any anomalies.
3. Hotlists -- Referencing information (devices, IP addresses, credit cards, debit cards, etc.) to both internal and external 'Hot' databases of stolen cards or compromised data (though the latter depends on the depth of coverage of those databases); and checking against EU and other Politically Exposed Person and terrorist lists.
4. Know Your Customer Checks (KYC) -- Proving that the information provided in an application or transaction is correct, namely that a person actually exists and resides where they say they do.
5. Variances -- Looking for changes between current and previous devices, I.P. locations and login sessions. If a customer usually logs in on their laptop from London, the e-gaming firm may question why they start logging in from an Internet café in Belgrade or Vietnam (though this may be because they are on a business trip or holiday).
6. Transaction Limits -- Use of limits to minimize the attractiveness of a business to fraudsters, thus reducing the value they can derive from one unique set of compromised information.
7. Velocity Thresholds -- Setting combinations of total spend over different time periods. This essentially creates 'Honey Traps' to pick up unusual patterns, which vary within the sector.
8. Unusual Data -- Looking for unusual changes of personal information on accounts, particularly in the early days of a new account. For an extreme example, it is unusual to open an account on the day one moves house, so why change the registered address as soon as the account is open?
9. Associations -- Looking for links between cards, bank accounts, I.P.s, devices and personal data. Fraudsters are unlikely to give up on the first attempt -- if a card has been used once already for a fraud, they may well try to use it again, though mostly in a short period before they consider that it may have been hot-listed. Peer-to-peer losses in poker and other games of skill are a particular source of risk and high customer cashouts are accompanied by alerts to double-check the hands that have been played, in addition to the routine expert monitoring of peer-to-peer games.
10. Verification -- Using systems such as Interactive Voice Response (IVR) to verify account applications or transaction history means that people can protect their business and the genuine consumer from identity theft or account takeover.

KNOW YOUR CUSTOMER (KYC)

INITIAL ACCEPTANCE

Controls over identity frauds are primarily the task of the financial services sector and retailers who hold sometimes unnecessarily large databases of card data and other personal information on customers, which, if compromised, can then be misused to facilitate identity frauds and money-laundering. There are particular problems of information-sharing between the financial and e-gaming sectors, and the e-gaming industry ignorance of the Bank Identification Number (BIN) ranges of pre-paid cards (which banks state they cannot provide) makes it hard to develop electronic checks to know whether or not a card is pre-paid and whether higher suspicion should attach to it and to transactions on it.

Detailed requirements and controls vary (as is reasonable under a risk-based approach to money laundering controls), but before a player can play for real money, customers may be required to provide the following information: Username, Password, E-mail address, First and Last names; Date of birth – the system does not accept a date of birth that would make the player less than 18 years of age; Sex; Address information; Country; Phone number; Account currency; Preferred contact Language; and Secret question and answer.

The amount of information available for verification varies in different European jurisdictions, depending on databases collected by governments and the private sector, and also the costs of verification.[30] Where possible, all real money players are verified electronically by external and internal systems to carry out age, ID and telephone verification (e.g. to check that the phone number they have given is not a professional services firm or is genuine). The telephone service telephones the number registered by the player and the player must enter the code displayed on his screen to confirm that the user is a real person with a real number. They verify that the name and address registered matches the name (last name and initial of the first name) and address of the person paying the telephone bill. The results of these verifications are put through a combined risk matrix, through which all players go on initial deposit. The category assigned determines whether or not the account requires further verification: if it does, those cases are outsourced to agents for review.

Some firms check to ensure that payment cards have not previously been registered with another player account, for multiple players sharing the same IP address, and for suspicious patterns of transactions. There is also a negative check against OFAC and EU lists of suspected terrorists as an (understandably) limited way of avoiding the financing of terrorism. It is accepted in official circles that terrorist finance typologies are not sufficiently well developed or widely communicated to serve as clear guidance beyond such lists.

ONGOING MONITORING

A variety of approaches take place for ongoing monitoring of accounts, once accepted. One firm has stated that up to 50 different automated checks are efficiently carried out to identify any suspicious behaviour during deposits and withdrawals, and analyzed by a team of experts. If suspicions are substantiated, the transactions relevant are cancelled and the accounts involved closed. No data are available as to how often this actually happens across the industry as a whole. Some firms employ staff from different countries speaking various languages, to enable them to test more rigorously whether or not conduct is suspicious and whether identity is properly established: this can be vital since models of suspicion developed for high-plastic societies (such as the UK) may not work in high-cash societies (such as much of Central and Eastern Europe).

To ensure efficient prevention of fraud, firms define a variety of characteristics of suspicious behaviour based on previous experience. They are automatically monitored each time a user makes a deposit before being

[30] For example banks charge for checks whether a particular card number is registered to a particular person, which drives up the costs of e-gaming and which e-gaming and other e-tailers are reluctant to pay unless they already have suspicions about customers, which happens with only a tiny proportion of total customers.

analyzed by the company's internal security team (some of which have been kept confidential for the purposes of this public report):

- initial deposits of substantial sums;
- deposits not immediately used as stakes in betting
- deposits and withdrawals made without placing any bets

If two or more characteristics of suspicious behaviour are detected and the company's representatives conclude that there are grounds for suspicion, the user's account is closed and deposits are returned.

Some firms monitor carefully all transactions over a moderate level (a balance between keeping the sum low enough to assist but not so small as to generate too many referrals and false positives), and other indicators of *prima facie* suspicious behaviour include people who in a short time make large winnings on sports betting after a small initial deposit. (Though the latter can turn out to be just good luck.)

The following transaction details can also be verified automatically:

- Does the country of origin of the credit card match the customer's country of registration?
- Does the country of origin of the normal IP address (PC identification) coincide with the customer's country of registration? (Though allowance has to be made for mobile gaming.)
- Do any details of the transaction (credit card number, IP address, etc.) appear in any 'hot' list?
- Is the same payment card being used by more than one customer?
- Is one customer using several credit cards or payment accounts?

A payment transaction can be denied if the response to two or more of the above questions is affirmative. In addition, checks for the following parameters automatically can be made to monitor the customer's behaviour since the deposit was made:

- small or no stake placed since deposit
- use of other payment options since last withdrawal
- use of other withdrawal options since last withdrawal

All of these can build up a pattern of information against which to assess the risks posed by particular customers. As in many areas of account opening and conduct, electronic profiling enables less costly judgments to be made about 'out of context' behaviour, though human intervention is always required to make threshold judgments about what course of action to pursue, and such human interventions constitute costs that are not in the narrow economic self-interest of e-gaming businesses, therefore being an effect of money laundering regulation and of corporate commitment to it.

COMPARISON WITH OTHER SECTORS

The UK and broader European payment card industry has a number of initiatives in place to counter e-commerce frauds:

- Visa and MasterCard have introduced secure payment systems (Verified by Visa and MasterCard SecureCode) for safer online transactions. Cardholders are prompted to register with Verified by Visa and MasterCard SecureCode whenever they shop online at a participating retailer's website.
- To pass this obstacle, cardholders need to register a private password with their card company for use when shopping online at participating retailers (and to remember it!) The systems also allow financial

institutions to verify for the retailer that a cardholder is genuine. More than 37 million cards – 26% of all UK cards – had already been registered for these systems by December 2008. (See www.becardsmart.org.uk.)

- An automated cardholder address verification (AVS) and card security code (CSC) system is available for businesses that accept phone, internet or mail order transactions in the UK. The system allows them to verify the billing address of a cardholder and cross-check the security code on the signature strip of the card. These data checks provide additional information to help e-gaming and other businesses assess fraud risks and decide whether to proceed with the transaction.

4. ASSESSING COMPLIANCE OF THE E-GAMING SECTOR WITH AML EFFORTS

In any area of compliance, a threshold judgment has to be made about how much compliance is 'good enough', and reasonable people can disagree about whether a particular set of facts or perceived facts constitutes adequate compliance. This sort of judgment is made at the country level by FATF and the FATF-style regional bodies – MoneyVal in the case of Europe – and at the sectoral level by national regulators and collective industry bodies. Compliance levels are properly seen in terms of a range rather than a binary category, but- as in the now terminated Non Cooperating Countries and Territories 'blacklisting' process at the beginning of the decade – countries, firms and individuals may have to be designated non-compliant and sanctions taken. For reasons of time, no attempt has been made in this study to carry out a *detailed* audit of compliance and of inter-firm consistency. Since we are focussing here upon the European regulated sector, compliance assessment is the task of the national regulators in jurisdictions where operators are licensed. However is plain that though procedures and control practices vary (as they do in all other regulated sectors such as financial services and the professions), genuine efforts are made by regulated e-gaming firms to identify customers and their suspicious behaviour, and there is reporting to Financial Intelligence Units of transactions and account behaviour that are deemed to be suspicious.

Laundering controls may be demarcated into 'front end' controls such as customer identification and 'back end' controls that may be deduced from patterns of trading and other aspects of the conduct of accounts. Arguably, in analyses of money-laundering issues and in evaluations, there has been too much focus historically upon the front end of customer identification rather than the more challenging back end customer monitoring compliance issues. On the former, given that they are utilising cards that have already been subject to KYC, further customer identification by regulated firms takes place on payouts above €2,000[31] - though major firms do so on *all* payouts - often subcontracted to European electronic verification firms; on the 'back end' compliance monitoring issues, many areas of e-gaming have an advantage because the modest scale of financial transactions and their predictability makes them easier to develop risk models for. E-gaming firms vary in the extent to which they impose spending limits, and in general business sectors and financial services, this would be regarded as a purely business decision, unless their solvency was threatened, which in this case would be very unlikely. Greater diligence is (and should be) exercised where gaming limits are higher, since this generates greater laundering opportunities. Land-based betting and gaming, though on the whole well regulated, have higher average and maximum spends, and our interviews suggest that high rollers prefer the ambience of off-line gambling, even where they also game online. Unlike cash-generating trading firms, however, the underlying transactions that form the basis of online gaming firms' accounts are transparent, verifiable in principle, and therefore e-gaming firms are difficult to use as front companies or as wilfully blind conduits for laundering, with or without senior management involvement.

REPORTING OF SUSPICIOUS TRANSACTIONS

One indicator of conformity with AML efforts might be thought to be the number of suspicious activity reports made to Financial Intelligence Units. Unfortunately this would be a serious error, since in itself, the number of reports is neither a success nor a failure indicator. First, the more effective front-line KYC and the less inherently exploitable an industry is to large post account-opening expansion of trading, the less likely a sector is to be used as a major money laundering conduit: subject to their skills and contacts, offenders will search for easier places to launder. Thus if money laundering controls are tight and are perceived by offenders to be tight (or are not contemplated at all by them as a laundering route), one might expect few SARs to be made.

[31] The threshold figure varies by jurisdiction, up to €3,000 in Alderney, depending on the interpretation given to the EC Third Directive.

On the other hand, in the absence of positive evidence of preventative effectiveness, the making of no or very few reports may reasonably be taken as an indicator that a sector is not making enough efforts to develop awareness and to pass on suspicions, including the rationale behind account termination, to Financial Intelligence Units.[32] Some SARs (though tiny in percentage terms) lead to the identification of previously unsuspected offenders, while a much larger number (though again a modest percentage) enhance the intelligence picture on criminal networks and proceeds of crime: but given constraints on financial investigation resources, sometimes fewer reports generate a better yield. In the UK in 2007-2008, out of a total of 210,052 SARs, the gaming sector made 403 SARs (up from 299 in 2006-07), of which 24 involved requests for consent to permit dealing with a person whose transactions they suspected of being proceeds of crime: however there is no breakdown for e-gaming compared with land-based gaming. By way of comparison, there were 33 reports direct from credit card companies,[33] and 280 reports from spread betting firms; 7,299 reports from money transmission firms, and 3,553 from bureaux de change.[34] One SAR from the gaming sector was considered sufficiently indicative to be transmitted to the National Terrorist Finance Unit for further investigation.

No data are available for sub-sectors EU-wide, though numbers of reports are inherently much lower in those countries where accounts are automatically frozen when a SAR is made. The numbers of SARs are not an index of vulnerability, but rather of activism by MLROs (which can include 'defensive reporting' to avoid criticism), so not much should be read into figures. To reiterate, a low number of SARs can mean either low risk (perhaps because good preventative action eliminates many attempts at source) or an industry 'in denial' about the risks that are generated; conversely a high number of SARs can mean that the industry is taking active steps to deal with problems, or that some or all firms are reporting suspicions without much analysis, either to disarm potential criticisms from regulators and the media for not reporting enough, or because they have insufficient compliance resources to carry out their internal review role properly.

CONCLUSIONS

The e-gaming industry uses a broad set of techniques to reduce the risks of fraud and of money-laundering, some of which make extremely sophisticated use of the data available in this technology-intensive area of leisure activity.[35] These include (to a variable extent):

- *Manual*

Agents flag cases they consider to be "suspicious" based on risk alerts, customer tip-offs and unusual betting and or wagering play by customers

- *Third Party Data*

Age Verification lists sourced from firms in the market

Hotlists, including the sorts of data sources used by banks to identify terrorists and foreign public officials who require 'Enhanced Due Diligence'

[32] The reporting to FIUs of suspicions which have led to the refusal to open an account is a contentious area of AML obligation generally.

[33] Credit card issuers in the UK obtained exemption from the requirement to submit SARs after every fraud, because to do so would place an unreasonable administrative burden for no obvious enforcement/intelligence benefit since, in most cases, there is no suspect.

[34] See the Serious and Organised Crime Agency (2008: 41).

[35] To avoid revealing information that may be useful to criminals, only broad outlines of measures have been detailed here. E-gaming using those Stored Value Cards (and, in the future, media such as payment-enabled mobile phones) that have *not* been through adequate KYC controls requires special attention, though not particularly by the e-gaming industry.

Telematching

The European Sports Security Association watch list

- *Rules Based*

Pre-defined rules based on business knowledge and past experiences. For example limitation on the number of credit cards that can be used; device reputation models

- *Statistical Profiling*

Outliers of transactional behaviour determined through regression analysis

Risk scoring models

- *Advanced Analytics – Artificial Intelligence*

Creating predictive modelling techniques

Implementation of neural networks to assist the human thought process in detecting fraudulent trends.

As with all business areas, there is scope for debate between directors, Money-Laundering Reporting Officers and regulators about levels of resources and best practice in keeping fraud and money-laundering risks down to 'acceptable' levels. (Though philosophically, it is arguable that those levels of fraud that are fully compensated by the gaming firms and do not risk insolvency are a matter for independent business decisions rather than for governments.[36]) It may be desirable to vary controls in order to keep criminals (with or without inside collusion) uncertain about what risks they face.

In short, compared to methods of customer identification and monitoring in the off-line gaming and financial services sector, the scope for substantial abuse of e-gaming for laundering purposes is modest, both for those crimes that generate cash and for those that do not. This is partly a result of the greater recording of transactions in this industry than in most others, and partly the consequence of legitimate firms being subject to regulation. There is doubtless scope for improvement in controls over fraud and laundering, and regulators need to be vigilant (i) about the levels of private sector resourcing of anti-fraud/AML efforts, without which risks would rise; and (ii) inter-jurisdictionally consistent in their requirements, following deliberation between regulators, preferably after consultation with the industry. However there is also much mythology about e-gaming laundering risks, which arises from inadequate information and a tendency to project a dislike of gaming and/or private sector involvement in it into alarm about e-crime. This report makes a start to this de-mythologising process, but crime and our responses to it are dynamic activities that require regular attention to trends if we are not to find ourselves stuck in a rut of fighting previous wars on crime. From a social benefit-cost perspective, the more desirable and realistic objective is to manage down the collateral harms generated by e-gaming opportunities, while preserving the liberty of those who wish to gamble and can afford to do so.

[36] On this principle, governments and regulators should intervene only where there is market failure or a serious risk of it. Even where compensation is paid to cardholders and/or gamblers for direct fraud losses, some externalities - economic and/or emotional costs - may fall upon those defrauded (Levi and Burrows, 2008).

REFERENCES

APACS (2009) *Fraud : the Facts 2009*, London : Association for Payment Clearing Services.

Bauer, A. (2008) *Jeux En Ligne et Menaces Criminelles*, Report for the *Ministre du Budget, des Comptes publics et de la Fonction publique*, Paris : Institut de Criminologie de Paris, Université de Paris II.

Cabinet Office/Home Office (2009) *Extending Our Reach: a Comprehensive Approach to Tackling Serious Organised Crime*, London Home Office.

Choo, R. (2008) 'Money laundering risks of prepaid stored value cards', *Trends and Issues in Crime and Criminal Justice No 363,* Canberra: Australian Institute of Criminology.

Choo, R. and Smith, R. (2008) 'Criminal Exploitation of Online Systems by Organised Crime Groups', *Asian Journal of Criminology* (2008) 3:37–59.

Europol (2005) *2005 EU Organised Crime Report - Public version*, 13788/1/05 REV 1 Crimeorg 117, The Hague: Europol.

Europol (2008) *EU Organised Crime Threat Assessment 2008*, The Hague: Europol.

FATF (2008a) *RBA Guidance for Casinos*, Paris: FATF.

FATF (2008b) *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems*, Paris: FATF.

FATF (2009) *Money-Laundering Through the Football Sector,* Paris: FATF.

FATF/APG (2009) *Vulnerabilities of Casinos and Gaming Sector*, Paris: FATF and Sydney: APG.

Levi, M. (2008) 'White-collar, organised and cyber crimes in the media: some contrasts and similarities', *Crime, Law and Social Change*, 49: 365–377.

Levi, M. (2009) 'Fear of Fraud and Fear of Crime: a Review', in S. Simpson and D. Weisburd (eds.) *The Criminology of White-Collar Crime*, New York: Springer.

Levi, M. and Burrows, J. (2008) 'Measuring the impact of fraud: a conceptual and empirical journey', *British Journal of Criminology*, 48(3): 293-318.

Levi, M. and Reuter, P. (2006) 'Money Laundering', in M. Tonry (ed.), *Crime and Justice: A Review of Research*, Vol.34: 289-375, Chicago: Chicago University Press.

MHA (2009) *The threat of money laundering and terrorist financing through the online gambling industry*, London: Remote Gambling Association.

Serious and Organised Crime Agency (2008) *The Suspicious Activity Reports Regime Annual Report 2008*, London: SOCA.

ANNEX 1 THE FATF REPORT ON CASINOS (2008)

Para. 8. “Internet casinos tend to only make/receive payments using accounts held by financial institutions”.

107. Internet casinos may wish to check customer location because of the additional risks arising from transnational operations”.

The report makes some systematic comparisons between risks arising in land-based and internet-based casinos:

109. Casinos should consider operational aspects (*i.e.* products, services, games, and accounts/account activities) that can be used to facilitate money laundering and terrorist financing activities. In addition, land-based and Internet casinos have the following potential transaction risks:

Proceeds of crime. However money is transferred to a casino, there is a risk that this money will have arisen from illegal activities such as check fraud, credit/debit card fraud, narcotics trafficking, theft from employer. Paying greater attention to high spenders/rollers will be helpful in mitigating this risk.

The majority of payments to Internet casinos are made directly from financial institution accounts. However, Internet casinos can operate as part of mixed gambling chains which also include betting shops and/or land-based casinos. It may be possible for customers to provide land-based outlets with cash which can then be credited to Internet casino accounts. Internet casinos should work closely with their land-based counterparts that initially receive the cash to ensure that CDD measures are applied, including verifying that the depositor is the account holder, and when appropriate, benefit is secured from the personal contact between land-based casino staff and customers.

Transfers between customers. If Internet casinos wish to allow inter- account transfers between their customers they should devise careful policies and procedures which monitor the amount of the transfer(s). Internet casinos may also be aware of customers transferring money between themselves more informally without using their casino accounts, which should be taken into consideration in the casino operator's risk assessments.

110. There are a number of specific transaction issues which apply to Internet casinos (including “mobile casinos”):

- *Multiple casino accounts or casino wallets*.

  An internet operator may own and control multiple web sites. Single web sites can also offer a range of different types of gambling. Operators will need to monitor customers' aggregate position across the whole of their casino business.
  Customers may wish to separate the different types of gambling they are conducting with the same operator, or through the same web site, for legitimate reasons, *e.g.* to monitor their performance in different areas. Casinos should implement procedures and systems to assist in the identification of customers opening multiple accounts or wallets for dishonest or inappropriate reasons, including attempting to obscure their spending levels, or to avoid checks undertaken at a threshold level.
- *Changes to financial institution accounts*. Casino customers commonly use their accounts with financial institutions to gamble over the internet. Customers may hold a number of financial institution accounts, and they may wish to change which of these accounts they use in the casino. Casinos may wish to consider updating customer due diligence following such changes.

- *Identity fraud*. Details of financial institution accounts may be stolen and used on web sites. Stolen identities may also be successfully used to open financial institutions accounts, and such accounts may also be used on web sites. Internet Provider (IP) Number checks are useful in preventing criminals from opening multiple casino accounts using stolen identities, using the same computer. Casinos will be aware of these risks because of the 'charge back' system. Internet casinos also have a responsibility to protect their customers from having their identities stolen when using their web site, and will therefore wish to provide adequate security.
- *Pre paid cards*. Using cash to fund a pre-paid card poses similar risks as cash. Casinos cannot make the same level of cross reference checks on some types of pre paid cards as they are able to perform on financial institution accounts.
- *Electronic wallets (e- wallets).* Not all e-wallets are licensed in reputable countries, and a number of e-wallets accept cash as deposits. However, e-wallets which only accept money from financial institution accounts in the customer's name will not usually pose any greater or lesser money laundering risk than if funds are received directly from the financial institution. However Internet casinos should be aware that when customers make payments into e-wallets from their financial institution accounts, the statements issued by their financial institutions may only record the payment to the e-wallet, not the transaction to the Internet casino. This may be useful for dishonest customers who wish to disguise their gambling. (See paragraph below regarding the related issue of casinos purposefully obscuring payments made to financial institution accounts held by customers).
- *Games involving multiple operators.* Poker games often take place on platforms (*i.e.* a central computer system that links electronic gambling devices for purposes of game selection, operation, monitoring, security, and auditing) shared by a number of different casino operators. The platform is likely to play a key role in monitoring the pattern and value of play for potential money laundering activities, *e.g.* chip dumping. The operator and the platform should have clear policies in respect to respective roles, alerts, enquiries, and subsequent actions, for AML/CFT.

121. Internet casinos may adopt specific methods of customer's identification. The FATF Recommendations recognise that non face to face business relationships or transactions can carry specific risks. For that reason non face to face business requires alternative or additional compliance methods, especially in the area of CDD. These methods may rely upon new technologies**,** including the deposit and withdrawal methods offered on the website, and checks on the customer's IP address.

122. In the majority of cases Internet casinos do not meet their clients, except perhaps their high spenders. Internet casinos are therefore usually unable to form social relationships with them, or to form judgements as a result of those relationships. They are also unable to verify customer's physical appearance against photographic identification documents.

123. If casinos use software systems to assist with CDD the software should access a range of positive and negative checks. Although not available in all countries, public source data can be particularly valuable in identifying PEP's and individuals subject to various sanctions, as well as identifying associations with organised crime and/or terrorist financing activities. In addition, casinos may wish to do Internet searches in an effort to obtain additional information about a customer (see also paragraph 138 below).

124. If basic database checks are not sufficient, perhaps because of a raised risk level, Internet casinos can use a variety of other checks: *i)* traditional checks using customer's personal and official documents; *ii)* checks on customers' source of funds; *iii)* using direct contact via telephone or email, using personal or electronic means.

128. With regard to Internet casinos, checks may be made on the location of the computer used when casino accounts are opened, or during gambling, including IP checks19. IP addresses provide information about the country where the computer being used is located.

129. It may be helpful to cross reference IP number information about jurisdiction with *i)* personal data provided by the player and the data provider by the Internet service provider; *ii)* the information the customer provides about their postal address and *iii)* if payment is made to the casino from a financial institution account, the country where the financial institution account is held, which may be ascertainable from a BIN check.

130. Internet casinos are dependent upon IT systems. These IT systems should be adapted to ensure accurate monitoring of accounts and customers, and to ensure that adequate records are kept and retained. Decisions may need to be made about the necessary level of details of the transaction records which are retained. A risk based approach cannot solely rely upon IT, there must also be an element of human supervision and staff levels should be proportionate to risk levels.