Cash Is Not King:
Thoughts on Financial Transactions in Internet Gaming

Stuart Hoegner*

1. A Framework for Investigating Financial Transactions & Standards

In almost any private enterprise, accepting value from customers—the 'consideration' in the transaction—is a key element of the contract and critical to the business's success. Most business owners likely do not give the issue much thought beyond the risk of fraud or counterfeiting. If the cash tendered is real, if the cheque is supported by the requisite funds, or if the credit card issuer allows the transaction, then the sale takes place. Seller and buyer are a*d idem* and each party gets what she wants.

In Internet gaming and betting, different considerations apply. For one thing, online interactive gaming, as with many other e-commerce channels, is a non-face-to-face business. Short of land-based marketing promotions or tournaments, operators will almost never meet their customers, or even speak with many of them by telephone. This has implications for, among other things, consumer protection measures and fraud prevention. The underlying activity (gaming and betting) is also problematic. Internet gaming has only been regulated for a few years. Much of the structure that is taken for granted in international bricks and mortar casinos, card rooms, and sports books is still emerging in online gaming, even in countries where i-gaming has been regulated for some time. Perhaps because of this, in the popular imagination the sector can be perceived as generating, or at least facilitating the transfer of, illicit proceeds.

Accordingly, it is worth discussing how to regulate transactions between licensed Internet gaming operators and their customers. This can be done through the prism of anti-money laundering initiatives. Money laundering provides a good framework for looking at financial transactions for two reasons. First, money laundering is likely the single biggest regulatory matter facing Internet gaming regulators from a transactional standpoint.[1] Se-

* CMA, LL.B. (Toronto), B.P.A. (Carleton), of the Ontario Bar. The author thanks the interview subjects for this paper as well as Karl F. Rutledge and Glenn J. Light for their valuable time, comments, and suggestions on the manuscript. Any errors in the article are, however, the author's alone.

cond, money laundering is emblematic of a larger transactional discussion. Money laundering draws in many of the issues and best practices that affect currency and transaction handling requirements more generally. It can serve as a means of focusing the discussion somewhat, while still generating feedback that goes beyond money laundering, *per se*. For example, many of the recommendations put forward here that prevent money laundering can also prevent consumer fraud. The standards adopted in this paper are also good practices for general financial transaction handling in online gaming and betting. For instance, good transaction processing protocols require proper identification of the transacting parties and a paper trail for subsequent audit and investigation, if that becomes necessary. Therefore, money laundering best practices will be our window onto good practices for currency and transaction handling writ large.

The discussion in this article will proceed under a number of discrete headings. Section 2 looks at defining the problem. A working definition of money laundering is adopted and its exclusions and limitations are set out. We also examine the various stages of money laundering and, critically, at why money laundering is important and worthy of discussion. Section 3 looks at the constraints on this analysis, including a lack of understanding about the precise size of the money laundering problem in online gaming and institutional and international barriers to any one regulator's effectiveness at combating it. Section 4 then proceeds to give a very brief and somewhat top line overview of the existing rules preventing money laundering as adopted by the Financial Action Task Force (the "**FATF**") and five jurisdictions that have elected to regulate Internet gaming: Alderney, the Isle of Man, Kahnawá:ke, Malta, and Nevada. Based upon this review and commentary, Section 5 sets out five key groups of recommended best practices in online interactive gaming to combat money laundering: regulating the sector; adopting a risk-based approach; ensuring parties are transparent; making transactions fully traceable; and, fostering the control and security of the gaming environment. Section 6 sets out two interesting payment facilities in current use (PayPal and Bitcoin) and tests each of them against the article's recommended standards to see how they fare.

2. Money Laundering and Why It Matters

Before embarking on a critique of current laws and a discussion of best practices to prevent money laundering in Internet gaming, one must settle on a definition of money laundering and how it typically works. What spe-

[1] Although, as we shall see in section 3.1, money laundering is probably not a particular problem in the Internet gaming and betting sector, and surely not any more so than any other e-commerce channel.

cific activity are we trying to prevent with the implementation of regulatory best practices? And why is it important to prevent money laundering?

The FATF states that money laundering is the processing of the proceeds associated with criminal acts in order to disguise their illegal origin.[2] Several competing—but broadly similar—definitions of money laundering are readily available.[3] Unsurprisingly, there is even a law and economics approach to money laundering characterizing it as a service satisfying a direct need and governed by the laws of supply and demand.[4]

Turning to definitions under national laws, it is an offence under the Canadian Criminal Code (the "**Code**") to, *inter alia*, use, send, deliver, transport, transmit, dispose of, or otherwise deal with proceeds or property with intent to conceal or convert those proceeds or that property, knowing that such proceeds or property derives directly or indirectly from a "designated offence" under the Code, *i.e.*, from an offence that may be prosecuted as an indictable offence under federal law; from a conspiracy to commit or attempting to commit such an indictable offence; or, from being an accessory after the fact to such an indictable offence.[5]

In the United States, one central definition of money laundering is found in title 18, section 1956 of the U.S. Code. Section 1956 "criminalizes virtually any dealings with proceeds from a range of specified unlawful activities when those dealings are aimed at furthering the same specified unlawful activities, or at concealing or disguising the source, ownership, location, or

---

[2] Financial Action Task Force, Money Laundering FAQ, *available at* http://www.fatf-gafi.org/document/29/0,3746,en_32250379_32235720_33659613_1_1_1_1,00.html.

[3] *See, e.g.* Anthony Cabot & Joseph Kelly, *Internet, Casinos and Money Laundering*, 2 J. Money Laundering Control 134 (1998); Andres Rueda, *The Implications of Strong Encryption Technology on Money Laundering*, 12 Alb. L.J. Sci. & Tech. 1, 7 (2001); Joseph M. Kelly & Mark Clayton, *Money Laundering and Land-Based Casinos*, 14 Gam. Law Rev. & Econ. 275 (2010); Mark D. Schopper, Comment, *Internet Gambling, Electronic Cash & Money Laundering: The Unintended Consequences of a Monetary Control Scheme*, 5 Chap. L. Rev. 303, 313 (2002); Jon Mills, *Internet Casinos: A Sure Bet for Money Laundering*, 19 Dick. J. Int'l L. 77, 78–79 (2000–2001); Alison S. Bachus, *From Drugs to Terrorism: The Focus in the International Fight Against Money Laundering After September 11, 2001*, 21 Ariz. J. Int'l & Comp. L. 835, 837 (2004); Amy Walters, Comment, *The Financial Action Task Force on Money Laundering: The World Strikes Back on Terrorist Financing*, 9 Law & Bus. Rev. Am. 167 (2003); Wendy J. Weimer, *Cyberlaundering: An International Cache for Microchip Money*, 13 DePaul Bus. L.J. 199, 203 (2000–2001); George Mangion, *Perspective from Malta: Money Laundering and Its Relation to Online Gambling*, 14 Gam. L. Rev. & Econ. 363 (2010); and, Roger C. Molander et al., Rand Corporation, Cyberpayments and Money Laundering: Problems and Promise xi (1998).

[4] Gál István László, *Some Thoughts About Money Laundering*, 139 Studia Iuridica Auctoritate Universitatis Pecs 167, 168 (2006).

[5] Criminal Code, R.S.C. ch. C-46 § 462.31(1) (1985).

nature of the proceeds."[6] (The issue of whether "proceeds" within the meaning of section 1956 refers to revenues ("receipts") or profits has been addressed by the U.S. Supreme Court. Instead of agreeing on a single definition of "proceeds" for all specified unlawful activities under federal law, the Court ratified both approaches, depending on the nature of the underlying offence.[7])

While many conceptions of money laundering are available from statutes, international recommendations, case law, and the academic literature, the definition used in the European Union's third Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing[8] (the "**Third Directive**") is both comprehensive enough to be meaningful and concise enough to be workable for our purposes. Article 1, section 2 of the Third Directive provides as follows:

> 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 counselling the commission of any of the actions mentioned in the foregoing points.

The definition of money laundering in the Third Directive is the definition that will be used in this paper.

This definition gives rise to two interesting issues that need to be addressed before proceeding: what to do about money laundering where the underlying gaming transaction is illegal under domestic law; and, whether combating the financing of terrorism is to be discussed.

The first concern is the legality or illegality of Internet gaming itself in any jurisdiction other than the licensing jurisdiction (if and where the two are different). If an online interactive operator conducts an illegal business

---

[6] Michael F. Zeldin & Richard W. Harms, *Anti-Money Laundering Compliance Programs: Principles from Traditional Financial Institutions Applied to Casinos*, 14 Gam. L. Rev 343, 344 (1997).

[7] United States v. Santos, 128 S.Ct. 2020 (2008).

[8] Commission Directive 2005/60, art. 1, 2005 O.J. (L 309) 15, 20.

in any particular place by taking the bet or wager, then Art. 1(2)(c) of the Third Directive may be engaged. The operator would be acquiring and using customer property (*i.e.*, funds) presumably knowing that those funds were derived from criminal activity. Or, as one scholar has put it:

> 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 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 (emphasis in original).[9]

The issue must at least be considered. To take a further example, if one were needed, consider prostitution. Assuming away issues of human trafficking, coercion, and power inequality does not get rid of the problem. Some states may see the avails of prostitution as criminal proceeds and bar dealing with them under money laundering statutes; other states may not. Certainly in a comparative law article, and especially one trying to set out best practices in Internet gaming, both the principle of comity and the different approaches to the underlying act of gambling itself need to be acknowledged.

An Internet gaming regulator can and, as a matter of principle, possibly *should* ensure that its interactive gaming licensees are accepting business only in jurisdictions in which accepting and transacting online bets and wagers is *not* a criminal act. The State of Nevada, for example, regulates intrastate online poker only; it should not be possible for a Nevada interactive gaming operator comporting itself pursuant to applicable local law to deal or transact in funds gained from an illegal bet or wager. There is no predicate gambling law violation because the interactive gaming that Nevada purports to regulate is legal, provided it is undertaken by state-licensed actors. No money laundering should be taking place, at least not because the bets or wagers themselves are criminal acts.

At the same time, it can be difficult for a regulator to make an assessment of whether a foreign bet or wager is legal or not. Aside from principle, the practical risk of over-regulation should also be acknowledged. In the

---

[9] Michael Levi, Money Laundering Risks and E-Gaming: A European Overview and Assessment—Final Report 13 (2009), *available at* http://www.egba.eu/pdf/Levi_Final_Money_Laundering_Risks_egaming%20280909.pdf.

words of one regulator, "there is an impact to everything that we do."[10] If Internet gaming regulatory standards are too low, then regulators run the risk of concern from and increased scrutiny and possible censure by the International Monetary Fund (the "**IMF**") and the FATF, among others. If regulatory standards are too high relative to other credible jurisdictions, a licensing body's stakeholders will complain.[11] There is a risk of pushing operators and consumers to more lightly-regulated places with lower compliance and transactions costs. This 'voting with their feet' effect can lower the overall international regulatory standard, thereby hurting the very consumers that the regulator seeks to protect in the first place.[12]

Is such a principled rule about definitively not allowing operators to accept business where the underlying bet or wager is or even may be illegal raising the standard "too high?" It is difficult to say. Nevada does it, but many others do not. For example, Rational Entertainment Enterprises Ltd. ("**Rational**"), the operator of www.pokerstars.com, is a licence holder in the Isle of Man.[13] Rational accepts wagers from customers in Canada, which may violate the relevant gaming provisions of the Code. Is Rational engaged in money laundering by these actions?[14] Again, an answer is elusive. Hypothetically, if the Isle of Man were to introduce a more invasive rule about the location of its licensees' customers, that may give a regulatory advantage to its competitors. Still, as Internet gaming becomes increasingly regulated by international bodies, the issue is bound to come up more and more; one suspects that the trend among regulators will be to accord increased respect to national laws and regulatory regimes and gradually shift towards prohibiting operators from taking business in states where the business itself is or even may be unlawful. In the meantime, many regulators will put the burden for making these decisions on their licence holders, which is both easy and, on some level, unsatisfying. At the same time, some operators will act unilaterally to publish and respect extensive restricted territories lists from which they will not accept gambling transactions.[15]

Though it is perhaps not ideal, for the balance of this paper, this aspect of the definition of money laundering will be set aside. Apart from the lack

---

[10] Interview with Steve Brennan, Chief Executive, Isle of Man Gambling Supervision Commission (Feb. 3, 2012) [hereinafter Brennan Interview].

[11] *Id.*

[12] *Id.*

[13] http://www.gov.im/gambling/licensees/.

[14] The Isle of Man Gambling Supervision Commission's position is that all operators must target markets that they are legally entitled to. If licensed operators are in any doubt, they are to take their own legal advice in the matter.

[15] *See, e.g.*
http://www.paddypower.com/bet/help?page=/al/12/2/article.aspx?aid=1566&tab=browse&bt=4&r=0.9481073

of unanimity among regulators on addressing this point, space limitations in this article do not allow for an in-depth discussion of the matter. A full treatment of the jurisdictional issues raised by this issue would require its own paper. We shall focus here on preventing Internet gaming operators from being used to launder criminal proceeds from sources other than the interactive gaming transactions themselves (if and where those transactions are unlawful).

The second issue is how to address combating the financing of terrorism. Until recently, the FATF had nine special recommendations designed to combat terrorist financing;[16] in February 2012, these nine special recommendations were merged into a recast set of 40 recommendations covering both money laundering and terrorist financing[17] (the "**40 Recommendations**"), but the terrorist financing concern remains central to the FATF's work.

Some of the safeguards used to prevent money laundering can also prevent the financing of terrorism. For example, as we shall see, part of knowing one's client should mean running a client name against the current Specially Designated Nationals List maintained by the Office of Foreign Assets Control (the "**OFAC**") in the U.S. Department of the Treasury. By its very nature, this exercise throws up a barrier to terrorist financing. However, terrorist financing and money laundering issues can be distinct. Money laundering is generally only more useful to criminal enterprises when larger amounts of cash or property are involved. Lower reporting or investigation thresholds restrain larger-scale money laundering. Different considerations can apply in terrorist financing, where even "very small amounts of laundering may be critical to terrorists' success."[18] For example, "an examination of the financial connections among September 11 hijackers showed that most of the individual transactions were small sums far below the reporting threshold and in most cases consisted only of wire transfers. The individuals

---

[16] Financial Action Task Force, FATF IX Special Recommendations (2008).

[17] Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation—The FATF Recommendations (2012), *available at* http://www.fatf-gafi.org/dataoecd/49/29/49684543.pdf [hereinafter 40 Recommendations].

[18] Levi, *supra* note 9, at 10. *See also* Interview with John Carlson, Principal Administrator, Financial Action Task Force (Feb. 1, 2012) [hereinafter Carlson Interview]; and, Michael Specter, *The Deadliest Virus*, The New Yorker, Mar. 12, 2012, at 36. (In the Specter article, the author addresses the threat of biological terror by means of a pandemic spread through a flu-like virus and states: "While scientists disagree sharply about whether it would be easy to replicate such a virus in a laboratory, and whether it would be worth the effort, there is no question that we are moving toward a time when work like this, and even more complex biology, will be accessible to anyone with the will to use it, a few basic chemicals, and a relatively small amount of money.")

appeared to be foreign students receiving money from their parents or grants for their studies."[19]

It is true that the FATF has not identified Internet gaming as a critical conduit for terrorist financing. There are many mechanisms used to get money to terrorists, and Internet gaming is not one of them.[20] (The *hawala* underground banking system in India and Pakistan appears to be a more noteworthy vehicle for Al Qaeda funding, for example.[21]) But, as the discussion will show, money laundering in regulated jurisdictions does not seem to be a particular problem now, either.[22] Perhaps the best way of addressing terrorist financing in Internet gaming is, for example, to mandate rigorous know your client ("**KYC**") standards in all cases and restrict payment processing to a few key banks regulated in a small number of first world states. However, there appears to be little appetite for adopting such tough standards.

The terrorist financing issue will be mostly set aside here. Some bulwarks can prevent both money laundering and terrorist financing. Given the relatively low reporting and enhanced customer due diligence thresholds for operators in certain Internet gaming jurisdictions compared to other participants in the financial system, other sectors and media seem to be more at risk. Furthermore, as terrorism can be financed by both legal and criminal activities, it may be that the scope or universe of behaviours necessary to generate such small amounts "is so vast that it is almost unmonitorable without sophisticated aggregate models and/or listing individuals and institutions believed to constitute such a threat."[23] In the context of a risk-based methodology, the risk in Internet gaming appears to be low. However, unless and until far stricter requirements are introduced, at least some conceptual risk probably remains.

The various stages of money laundering—the more specific process through which property is converted or transferred and its attendant transactions concealed and disguised—are often referred to as the placement,

---

[19] Walters, *supra* note 3, at 178–179.

[20] Carlson Interview, *supra* note 18. Also note the comments of Frank Catania, former Director of the New Jersey Division of Gaming Enforcement, from 2001: "No one at any level in law enforcement has ever alleged, asserted, or, as far as I know, theorized, that terrorist organizations have ever used on-line gaming to launder money." T*estimony of Frank Catania: Hearing on H.R. 556 and H.R. 3215 Before the H. Subcomm. on Crime*, 107th Cong. (2001).

[21] *Compare* Walters, *supra* note 3, at 171.

[22] *See generally* Evan Osnos, *The God of Gamblers: Why Las Vegas is moving to Macau*, The New Yorker, Apr. 9, 2012, at 49. (Osnos avers that land-based casinos are part of a widespread money laundering problem in Macau; one source calls Macau "a cesspool" of financial crimes.)

[23] Levi, *supra* note 8, at 10. (As with the Specially Designated Nationals List at OFAC, such a list—while perhaps not capable of distilling all international terrorist threats—can be maintained and should be checked.)

layering, and integration stages.[24] The placement stage involves the movement of proceeds—almost invariably cash[25]—from criminal undertakings into the financial system. Conceptually, this may be as straightforward as a deposit of illegal drug profits into a bank account or the purchase of chips at a casino table game using small denomination bills.[26] The placement phase "is the most vulnerable to law enforcement detection because it involves the physical disposal of cash."[27] As we shall see, the resistance to cash as a deposit method on Internet gaming websites (except when it is deposited indirectly by credit or debit card through a licensed financial institution) serves as a bulwark against the use of Internet gaming site operators to place funds at this stage of the laundry. However, a barrier like this could be threatened by payment solutions that provide, for example, anonymity for their users;[28] the problem of anonymous users will be addressed in later sections of this paper on best practices and on selected risk factors in Internet gaming.

After funds have been placed into the financial system, the money launderer generally engages in a series of transfers and conversions of the illicit funds in the layering stage. These movements—or 'layering' of multiple transactions—are intended to distance the originating proceeds from their source,[29] disguise their owner, and obscure the money trail.[30] This stage is seen as the most international and complex phase of the laundry cycle as funds are typically moved around multiple foreign accounts.[31] An example of layering is the transmission of illegal funds from one bank to a different bank in another country, followed by investing and moving the funds within a foreign market to avoid detection.[32] Understanding the justification for currency movements and adopting standards prohibiting or calling for the reporting of suspicious transactions can prevent Internet gaming operators from being used to layer transactions. These measures will also be addressed later in the discussion.

---

[24] *See, e.g.* Financial Action Task Force, Money Laundering FAQ, *supra* note 2; Cabot & Kelly, *supra* note 3, at 134; Rueda, *supra* note 3, at 88–91; Bachus, *supra* note 3, at 842–845; and, Schopper, *supra* note 3, at 313.

[25] *See* Ping He, *A typological study on money laundering*, 13 J. Money Laundering Control 15, 16 (2010); MHA Consulting, The threat of money laundering through the online gambling industry 5 (2009), *available at* http://www.rga.eu.com/data/files/final__mha_report_june_2009.pdf [hereinafter MHA Report].

[26] *See* Cabot & Kelly, *supra* note 3, at 141.

[27] Bachus, *supra* note 3, at 842.

[28] Rueda, *supra* note 3, at 88.

[29] Financial Action Task Force, Money Laundering FAQ, *supra* note 2.

[30] Bachus, *supra* note 3, at 844.

[31] *Id.*

[32] *Id.*

Finally, integration is the folded clothes of the money laundry. In this stage, "funds re-enter the legitimate economy."[33] For example, after entering the financial system and a series of movements to obfuscate the source of funds and ownership, a money launderer or her accomplice might withdraw funds from a bank account or investment account and uses them in the legitimate economy or for purchases to fuel further illegal activity and profits.[34] Here again, Internet gaming operators' aversion to cash transactions and the propensity to send withdrawals to licensed intermediaries provides a check on this part of the laundry cycle, but anonymity can cut against this barrier. Proper rules governing withdrawals, peer-to-peer transactions, and anonymity can curb integration. These items will be discussed later in the paper.

With the 'what' addressed, we turn to the 'why:' Why does money laundering matter? Why do we—or should we—care? There are at least three answers: money laundering undermines the rule of law; money laundering negatively impacts business; and, money laundering impedes economic development.

First, money laundering undermines the rule of law. Allowing money laundering to go on unchecked permits criminals to enjoy the spoils of their illicit activity and use their profits to potentially pursue new illegal activities. In a very real sense, money laundering can make crime pay. It can also allow for criminal elements to acquire large sectors of an economy and corrupt public officials through the laundry.[35] This has the potential to foster "an environment where criminal activity permeates a country's economic and political system,"[36] thereby undermining trust in and respect for the law.

Money laundering also hurts business. Widespread money laundering can draw businesses into its web and make them complicit in criminality, even unwittingly.[37] By undermining the financial system, money laundering may also foment a lack of confidence by business in a state's institutions. Because honest business people may not know which institutions to trust in a place where money laundering is rife, they may decline investment and cut off credit. The FATF cites volatility in money demand and international capital flows and risks to bank soundness among further business risks.[38] This instability and uncertainty stifles production and increases transactions costs to businesses and consumers.

---

[33] Financial Action Task Force, Money Laundering FAQ, *supra* note 2.
[34] See Bachus, *supra* note 3, at 845.
[35] Financial Action Task Force, Money Laundering FAQ, *supra* note 2.
[36] Bachus, *supra* note 3, at 841.
[37] Financial Action Task Force, Money Laundering FAQ, *supra* note 2.
[38] *Id.*

Finally, money laundering hinders economic development. Shrinking businesses means falling aggregate output on a macroeconomic level. Partly as a result of the effects on businesses and society, widespread money laundering harms the potential economic development of any state because honest, long-term investors are loath to invest in economies fuelled by illicit funds.[39]

We have settled on a working definition of money laundering for the analysis that follows. This definition will exclude proceeds from taking Internet bets or wagers where such transactions are criminal acts pursuant to national law. The following analysis will also not particularly address combating the financing of terrorism. The stages of money laundering have been briefly described, as have its insidious effects and costs. Now we shall examine some limitations on our ambitions for creating a template for best practices in addressing transaction handling and suppressing money laundering.

3. Even Best Practices are Constrained

There is only so far that best practices for preventing money laundering can go. We do not know the extent of the money laundering problem associated with Internet gaming. Money laundering is also an international, multi-faceted, and multi-institutional issue. The best practices of one actor, or even one state, can be expected to make only a limited difference. The various constraints on what are known about money laundering and on what regulators are—or each regulator is—capable of doing must be explained and acknowledged before reviewing current applicable safeguards and formulating a prescriptive approach to the issues.

3.1. The Size of the Problem is Unclear

Estimates of the size of the global money laundering problem vary. Several years ago, some said that in absolute dollar terms somewhere between US$300 billion and US$500 billion were laundered internationally each year.[40] More recently, others have suggested that the problem is quantitatively bigger, and that worldwide money laundering was valued at from US$590 billion to US$1.5 trillion annually, or between two and five per cent of the world's aggregate gross domestic product.[41] This latter range relies upon data put together by the IMF based on 1996 figures.[42]

The FATF states "that overall it is absolutely impossible to produce a reliable estimate of the amount of money laundered and therefore the FATF

[39] Bachus, *supra* note 3, at 841.
[40] Cabot & Kelly, *supra* note 3, at 134; Mills, *supra* note 3, at 78.
[41] Bachus, *supra* note 3, at 835; László, *supra* note 4, at 167.
[42] Financial Action Task Force, Money Laundering FAQ, *supra* note 2.

does not publish any figures in this regard."[43] It is exceedingly difficult to measure the size of money laundering. Key problems making it hard to quantify include the lack of recording of basic statistics, estimation problems around undiscovered criminality, and the emphasis on proving guilt over demonstrating the proceeds or profits from crime.[44] However, "[w]hat one can say with a reasonable degree of confidence is that the proceeds of serious crime that is generated annually globally is going to be a large number running into the hundreds of billions of dollars. While you may not be able to come up with a precise number, it's significant."[45] There is no better figure available than the IMF estimate of 2-5% of global GDP.[46]

The problem is with measuring the size of money laundering in regulated Internet gaming as a subset of global money laundering across all channels. There is no readily available estimate of the amount of laundering committed using Internet gaming facilities. Respective money laundering and Internet gaming experts are not aware of any figures quantifying it.[47] A reliable estimate may simply not exist.

In the absence of a quantitative estimate of the size of money laundering attributable to online interactive gaming, what should we conclude about the scope of the problem, if any? How big is it? The answer may be: not very.

Many commentators fairly presenting the risks and concerns about Internet gaming as a money laundering channel either cite conceptual concerns without any quantitative evidence—which seems appropriate, as the quantitative evidence does not appear to exist—or pitch their concerns with so many qualifications that no reasonable person would disagree. For instance, one article cites "many prosecutors agree[ing] that it is easy and economical to launder criminal proceeds through offshore casinos"[48] without any particular discussion of how exactly the proceeds are laundered, whether this includes regulated and unregulated regimes, or what particular offshore jurisdictions cause concern. Another example: The (unenacted) Unlawful Internet Gambling Funding Prohibition Act[49] (the "**UIGFPA**") listed the following as a congressional finding: "Internet gambling conducted through offshore jurisdictions has been identified by United States law en-

---

[43] *Id.*
[44] Carlson Interview, supra note 18.
[45] *Id.*
[46] *Id.*
[47] *Id.*; Brennan Interview, supra note 10.
[48] Mills, *supra* note 3, at 78.
[49] H.R. 556, 107th Cong (2001).

forcement officials as a significant money laundering vulnerability."[50] But again, there is no discussion of the amount of proceeds caught up in the alleged laundry.

Furthermore, Jonathan Gottfried posits as follows: "Unregulated Internet casinos may pose several money-laundering risks, particularly at the layering stage. The speed, international character, and possible anonymity of certain Internet gambling transactions, together with the potential of transferring large sums of money, may attract money launderers to online gambling operations."[51] For one thing, no-one is seriously suggesting that Internet gaming should not be regulated; as this article will show, appropriate regulation of the industry is a *sine qua non* preventing money laundering. For another, most are seemingly not advocating player anonymity, especially as regards the transfer of "large sums of money." Of course such an un- or under-regulated environment allowing for anonymity "may" attract risks of money laundering and criminal elements. That seems axiomatic. It is just not generally what is being proposed by serious proponents of Internet gaming regulation.

Others have arrived at more nuanced and less alarmist formulations. Almost fifteen years ago, Anthony Cabot and Joseph Kelly stated that "[t]he connection between money laundering and Internet gambling is one of the most complex issues facing regulators,"[52] which was undoubtedly true in 1998 and is quite likely true today. Two years later, the U.S. Congress's General Accounting Office (now the Government Accountability Office) (the "**GAO**") reported to Congress on some of the issues in Internet gaming.[53] The report noted that representatives of law enforcement ex-

---

[50] *Id.* at § 2(4). *See also* Schopper, *supra* note 3, at 311, citing this provision of the UIGFPA. Note that this finding was absent from the Unlawful Internet Gambling Enforcement Act of 2006 § 802, 31 U.S.C. §§ 5361–5367 (2006).

[51] Jonathan Gottfried, *The Federal Framework for Internet Gambling*, 10 Rich. J.L. & Tech. 26, ¶ 20 (2004), *available at* http://law.richmond.edu/jolt/v10i3/article26.pdf. *Compare* Jonathan Schwartz, *Click the Mouse and Bet the House: The United States' Internet Gambling Restrictions Before the World Trade Organization*, 2005 U. Ill. J.L. Tech. & Pol'y 125, 130 (2005), citing Gottfried.

[52] Cabot & Kelly, *supra* note 3, at 144. They also cite a 1998 FATF annual report with regard to concerns about money laundering through Internet casinos in "several countries" offering "complete anonymity to potential gamblers … placing their bets by way of credit card." Financial Action Task Force, Annual Report 1997–1998 47 (1998). As will be shown, the FATF now has specific recommendations covering Internet gaming operators. If regulators are fully implementing those recommendations and their own controls, *quaere* how applicable those concerns are today. Note also that "several countries" should not be taken as impugning all countries. Finally, remember that neither this article nor any reasonable observer is advocating complete anonymity, though it is not exactly clear how complete player anonymity is ever obtained through the use of a legitimate credit card possessed by the player.

[53] U.S. Gen. Accounting Office, Internet Gambling: An Overview of the Issues (2002), *available at* http://www.gao.gov/new.items/d0389.pdf.

pressed concerns that Internet gaming could be a "powerful vehicle for laundering criminal proceeds."[54] At the same time, law enforcement officials conceded that there was a lack of adjudicated cases involving money laundering through Internet gaming sites.[55] By contrast, banking representatives and gaming regulators did not view Internet gaming as particularly susceptible to—or as posing any particular risks in respect of—money laundering.[56] The GAO report made no recommendations to Congress.

On the other hand, several experts are not shy about forcefully and convincingly arguing that money laundering is not much of a problem in regulated Internet gaming. Some paint with a wide brush and offer little discussion in respect of their assertions and conclusions.[57] However, there are others offering thoughtful reasoning about why money laundering is not a particularly material issue in regulated online gaming.[58]

For example, in a money laundering roundtable from three years ago,[59] several gaming experts discussed whether they were aware of any evidence of money laundering by means of the Internet in any global jurisdiction. Frank Catania said that he had not seen any such evidence.[60] Alan Pedley, an Internet gaming expert and former regulator, indicated that he had seen one instance in Australia, but that the vulnerabilities leading to that instance had been addressed and corrected. Pedley added that he had encountered historical opportunities for money laundering that had since been "plugged," *i.e.*, addressed.[61] Mark Clayton, a gaming attorney in Nevada and former member of the Nevada Gaming Control Board, concluded that he agreed with the previous comments in the roundtable suggesting "that Internet gaming properly regulated is already difficult to launder money through."[62]

In the MHA Report from 2009, the authors conclude that "there appears to be little evidence to support the view that remote gambling has, to date being [*sic*] particularly susceptible to money laundering and terrorist financing. The United States has published the results of official government studies concluding that online gambling is not a likely accessible avenue for

---

[54] *Id.* at 5.

[55] This was said to be, in part, because of a "lack of *any* industry regulations or oversight (emphasis added)." *Id.*

[56] *Id.*

[57] *See, e.g.* Mangion, *supra* note 3, at 363: "Interestingly, statistics prove that online gaming is less prone to money laundering than land-based gambling in venues such as casinos and on a race track." (No such statistics are cited.)

[58] *See, e.g.* Sue Schneider, *Money Laundering and Terrorist Financing in the I-Gaming World*, 14 Gam. L. Rev. & Econ. 657 (2010).

[59] Joseph M. Kelly et al, *How Vigilant Should We Be against Money Laundering?* 13 Gam. L. Rev. & Econ. 278 (2009).

[60] *Id.* at 280.

[61] *Id.*

[62] *Id.* at 282.

money laundering."[63] This is because the identities of gamblers are known, financial transactions are in electronic formats, and all of the wagering is recorded.[64] Put another way, the money laundering risks associated with Internet gaming "are comparatively modest, due to the high traceability of e-gaming transactions and the customer identification controls in the regulated sector."[65] Accordingly, it appears that, while money laundering in regulated i-gaming is worth the effort to discuss and to implement best practices, there is little evidence of it being a serious problem and, in fact, the risk of it happening in regulated markets is likely low.

All of these perspectives and data points are important because regulating Internet gaming—and implementing sound financial transaction handling rules—is fundamentally a public policy issue. In any question about policy, it should be a key to understanding the issues to know what the size of the problem is, if it is a problem at all. To use a crude analogy, traffic fatalities on modern roads could likely be reduced by lowering the speed limit, but that interferes with the convenience of going faster and reducing travel times for other motorists. How many lives is it worth for all of us to go faster?[66]

In Internet gaming, how inconvenienced and compliance-focused must we be so that we can prevent money laundering? Doesn't the answer depend on the size of the money laundering problem in online interactive gaming? The point is that a discussion about costs of regulation versus the costs of the problem is in order. Does regulated Internet gaming account for half of the money laundering undertaken worldwide? Eighty per cent? Or, as seems likely, does it make up a very small amount? If regulated Internet gaming is the vehicle through which a substantial amount of money is laundered, then public policy makers are signalled that more resources must be allocated to prevent it. If next to nothing goes through a regulated i-gaming laundry, then that also conveys information about: a) the current efficacy of anti-money laundering protocols; and, b) what other resources, if any, need to be devoted to the problem.

Not having a working quantitative estimate is no reason to ignore the issue. However, it is only responsible to face the fact that, in the absence of a reliable measure about the amount of money laundering in interactive gaming, we are proceeding without useful—if not critical—information to determine how many resources to allocate to fund rule-making, investigations,

---

[63] MHA Report, *supra* note 25, at 31.

[64] *Id.*

[65] Levi, *supra* note 9, at 4.

[66] *See* Orley Ashenfelter & Michael Greenstone, National Bureau of Economic Research, Using Mandated Speed Limits to Measure the Value of a Statistical Life (2002), *available at* http://www.nber.org/papers/w9094.pdf.

and ongoing compliance, *i.e.*, to fund the legal and institutional machinery to prevent money laundering in the sector.

3.2. One Regulator's Effectiveness is Limited

The second set of constraints on the effectiveness of regulators in this area has to do with interconnectedness: money laundering is an international and multi-institutional problem. Moreover, preventing money laundering relies on multiple functionalities, some of which will not be discussed in this paper.

First, money laundering is, as recognized by the Third Directive, "frequently carried out in an international context."[67] As noted by the FATF, differences between national anti-money laundering regimes will be exploited by launderers, who will move their networks and operations to states and financial systems with weak or ineffective countermeasures.[68] The movement of capital—facilitated by modern technology—over ever more porous borders makes this continuous searching by criminal elements for the path of least resistance inherently global. Moreover, from an exclusively investigative standpoint, tracking flows of cash through financial institutions seems almost invariably an international exercise. Effective money laundering investigations and prosecutions require the co-operation of any number of foreign governments.[69] Accordingly, an Internet gaming regulator with all of the best proven methods for deterring money laundering is potentially still at the mercy of the weakest link in a global financial chain. As we shall see, bad actors in the financial system can be shut out of transactions based upon risk, but the exposure and limitation fundamentally remains: any regulator will be constrained in its effectiveness by the global nature of both Internet gaming and money laundering.

Second, regulatory effectiveness depends on multiple institutions. Even forgetting about the international context, the interconnectedness of financial institutions, regulators, and intermediaries at a national level precludes any one institution from providing a complete solution to the problem. For instance, if a gaming regulator has stringent controls on financial institutions with whom its Internet gaming operators may deal, but the same state's banks experience a breakdown of their respective money laundering controls, then the operators could potentially become part of an illicit laun-

---

[67] Commission Directive 2005/60, art. 1, 2005 O.J. (L 309) 15.

[68] Financial Action Task Force, Money Laundering FAQ, *supra* note 2.

[69] Mills, *supra* note 3, at 84–85; Bachus, *supra* note 3, at 773.

dry. Such a cross-institutional perspective is effectively adopted by the IMF in its various country reports.[70]

Finally, anti-money laundering controls appeal to multiple typologies, not all of which can be usefully covered in this paper. This point can seem abstract, but consider some specific ways different factors can affect the fight against laundering. Clearly things like cash limits on transactions, assessments of suitability, control over local operating nexus, and the act of gaming regulation itself affect money laundering. These will be addressed later. But what of something like location verification? As we will see, this can be a serious risk factor for money laundering, for example, where a customer's location is a country on the FATF's list of jurisdictions requiring counter-measures or its deficiencies list. Location verification, however, will be addressed in detail in another part of this volume. Or consider an Internet gaming site's random number generator ("**RNG**") on selected games. With a corrupted RNG, it is possible to turn a gaming website into a laundering vehicle for selected players or members of the operator's staff.[71] Here again, however, those kinds of fraud and technology issues will be addressed in other contexts and not in this paper. Still, it is important to note that our analysis will be limited by dealing with narrower functions and exposures on online interactive websites.

Having looked briefly at the broad restrictions on the effectiveness of an Internet gaming regulator—because the size of money laundering associated with regulated Internet gaming is unknown and because of the international, multi-institutional, and multi-disciplinary issues—the article will move to a discussion of comparative law. Fundamentally, what are the various rules, restrictions, and procedures in place in different international online gaming jurisdictions that can inform our search for best practices for financial transaction handling?

4. What are the Rules?

In this section, we examine how sundry international jurisdictions approach legal and secure financial transaction handling with a view to preventing their charges from becoming machines in an illicit laundry. The discussion starts with a look at the background and current makeup of the FATF followed by a review of their 40 Recommendations. The section then

---

[70] *See, e.g.* International Monetary Fund, IMF Country Report 09/278, Isle of Man: Financial Sector Assessment Program Update—Detailed Assessment of Observance of AML/CFT (2009), *available at* http://www.imf.org/external/pubs/ft/scr/2009/cr09278.pdf [hereinafter IMF Isle of Man Report].

[71] *See* Cabot & Kelly, *supra* note 3, at 144.

proceeds to canvass five jurisdictions to see how they approach money laundering controls in online interactive gaming: Alderney, the Isle of Man, Kahnawá:ke, Malta, and Nevada. Each of these will be looked at with specific reference to some of the following characteristics: suitability; customer identification and verification through due diligence; continuous monitoring; suspicious transaction reporting; record and data retention; tipping-off; and relationships with financial and payment intermediaries. This comparative review will form the basis for the bulk of the recommendations for best practices presented in the next section.

4.1. The FATF and the 40 Recommendations

The FATF is a body that was established by the G7 countries (as they then were) in 1989.[72] The FATF was convened in response to mounting concern about global money laundering,[73] and "was given the responsibility of examining money laundering techniques and trends, reviewing the action which had already been taken at a national or international level, and setting out the measures that still needed to be taken to combat money laundering."[74] The FATF's current mandate is four-fold:

1. to deepen global surveillance of evolving criminal and terrorist threats that it identifies;
2. to respond to new threats that affect the integrity of the financial systems such as proliferation finance;
3. to build a stronger, practical, and ongoing partnership with the private sector at the front line of the global fight against money launderers and terrorist financiers; and,
4. to support global efforts to raise standards, especially in so-called 'low capacity' countries.[75]

Today, the FATF continues to develop and promote policies to combat money laundering and terrorist financing.[76] This it does through, *inter alia*,

---

[72] Financial Action Task Force, About the FATF, *available at* http://www.fatf-gafi.org/pages/0,3417,en_32250379_32236836_1_1_1_1_1,00.html. *See also* Walters, *supra* note 3, at 168; Rueda, *supra* note 3, at 15–16; and, Alan E. Sorcher, *Lost In Implementation: Financial Institutions Face Challenges Complying With Anti-Money Laundering Laws*, 18 Transnat'l Law 395, 405 (2005).

[73] Financial Action Task Force, About the FATF, *supra* note 72. *See also* Walters, *supra* note 3, at 168.

[74] Financial Action Task Force, About the FATF, *supra* note 72.

[75] Financial Action Task Force, FATF Revised Mandate 2008–2012, *available at* http://www.fatf-gafi.org/document/10/0,3746,en_32250379_32236836_40433674_1_1_1_1,00.html.

[76] Financial Action Task Force, About the FATF, *supra* note 72.

regularly revising the 40 Recommendations and their respective interpretive notes and by conducting evaluations of countries and industries to monitor and assess their compliance with the 40 Recommendations; these two broad functions are likely the two most significant areas of current activity for the FATF.[77]

There are currently 36 members of the FATF: 34 jurisdictions and two international organizations (the Gulf Co-operation Council and the European Commission).[78] The FATF works closely with eight regional bodies that are FATF associate members.[79] The associate members work to combat money laundering and terrorist financing in various regions. The FATF also has many observers, including the United Nations, the IMF, the World Bank, and the Organization for Economic Co-operation and Development.

The FATF's work has been called instrumental in co-ordinating the fight against global money laundering.[80] Perhaps because of the FATF's specialization (expressed in its mandate, for example), the depth of its membership, and the importance placed on its work by its members, among other factors, its 40 Recommendations represent *the* accepted international standard for anti-money laundering principles and procedures and have been adopted or endorsed by many nations and international bodies.[81] They "are the most comprehensive set of anti-money laundering directives yet created for governments, legislatures, law enforcement, financial institutions and businesses."[82]

The FATF issued a series of recommendations in 1990 to combat money laundering.[83] These were subsequently revised in 1996 and 2003,[84] but the process of revision and review is ongoing. In 2001, in response to an expanded mandate, the FATF issued eight special recommendations against terrorist financing; a ninth was added in 2004.[85] Until 2012, these collective

---

[77] Carlson Interview, *supra* note 18.

[78] Financial Action Task Force, FATF Members and Observers, *available at* http://www.fatf-gafi.org/document/52/0,3746,en_32250379_32236869_34027188_1_1_1_1,00.html.

[79] *Id*.

[80] Rueda, *supra* note 3, at 16.

[81] Sorcher, *supra* note 72, at 406; Walters, *supra* note 3, at 169; Department of Finance Canada, Strengthening Canada's Anti-Money Laundering and Anti-Terrorist Financing Regime, Consultation Paper 1 (2011), *available at* http://www.fin.gc.ca/activty/consult/pcmltfa-lrpcfat-eng.pdf.

[82] Walters, *supra* note 3, at 169.

[83] Financial Action Task Force, The 40 Recommendations, *available at* http://www.fatf-gafi.org/document/28/0,3746,en_32250379_32236920_33658140_1_1_1_1,00.html#40recs.

[84] *Id. See also* Financial Action Task Force, FATF 40 Recommendations (2003), *available at* http://www.fatf-gafi.org/dataoecd/7/40/34849567.PDF.

[85] Financial Action Task Force, Terrorist Financing, *available at* http://www.fatf-

recommendations were called the '40+9.' As mentioned previously,[86] all of the FATF's recommendations have now been consolidated into the (current) 40 Recommendations.[87]

The FATF recommends a risk-based approach to money laundering. This is enshrined in the first of the 40 Recommendations.[88] But what does this mean? The risk-based approach refers to identifying and assessing the risks of money laundering and terrorist financing by individual countries and, based on that assessment, ensuring "that measures to prevent or mitigate money laundering and terrorist financing are commensurate with the risks identified … Where countries identify higher risks, they should ensure that their AML/CFT [anti-money laundering and countering the financing of terrorism] regime adequately addresses such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the FATF Recommendations under certain circumstances."[89] The FATF calls this approach an "essential foundation" for efficiently allocating resources and implementing the 40 Recommendations.[90] The risk-based approach is a key part of the guidance for casinos issued by the FATF in 2008.[91] More will be said about issues raised by the risk-based approach in section 5.2, below, but it is currently mandated by several global Internet gaming regulators and it forms a key part of practices recommended by this article.

The 40 Recommendations expressly include and apply to Internet casinos. So-called designated non-financial businesses and professionals ("**DNFBPs**") in the 40 Recommendations include casinos and, in a footnote, the FATF clarifies that references to "casinos" include "Internet casinos."[92] Accordingly, recommendation number 22 sets out that the customer

---

gafi.org/pages/0,3417,en_32250379_32236947_1_1_1_1_1,00.html. *See also* Financial Action Task Force, FATF IX Special Recommendations (2008), *supra* note 17.

[86] *See supra* text accompanying note 15.

[87] Financial Action Task Force, 40 Recommendations, *supra* note 17.

[88] *Id.* at 11.

[89] *Id.*

[90] *Id.*

[91] Financial Action Task Force, RBA Guidance for Casinos (2008), *available at* http://www.fatf-gafi.org/dataoecd/5/61/41584370.pdf.

[92] Financial Action Task Force, 40 Recommendations, *supra* note 17, at 113. The 40 Recommendations do not distinguish between Internet casinos, Internet bookmakers, Internet poker rooms, or other types of Internet betting or gaming. However, there is little reason to suppose that very similar anti-money laundering policy concerns would not apply across all of these channels. In each case, funds are being wagered on participating in various games or external contingencies. With respect to games, this is so whether the games are house-banked (*e.g.*, craps) or not (*e.g.*, poker). The FATF has left it to individual countries to further define "Internet casinos" using a risk-based approach. In practice, however, the FATF believes that "Internet casinos" would likely include all above-mentioned types of Internet gaming and

due diligence and record-keeping requirements in recommendations 10, 11, 12, 15, and 17 apply to casinos, including Internet casinos.[93] Recommendation 23 provides that the provisions on internal controls, foreign branches and subsidiaries, higher-risk countries, suspicious transaction reporting, tipping-off, and confidentiality in recommendations 18–21, inclusive, all apply to casinos and, by extension, to Internet casinos.[94] In addition, recommendation 28 states that DNFBPs should be subject to regulation and supervision; this includes assessing the suitability of Internet casino owners.[95] Finally, recommendation 14 provides that providers of money or value transfer services ("**MVTS**") should be licensed or regulated and compliant with relevant FATF recommendations.[96] MVTS businesses are businesses that accept cash and other monetary instruments or other stores of value and then pay corresponding sums in cash or in other forms to a beneficiary.[97] The MVTS definition clearly includes a service like PayPal, for example.

Most of the FATF recommendations relevant to this paper are summarized in Table 1.

---

betting. Accordingly, all references herein to "Internet casinos" will be taken to include all of these wagering options and operations.

[93] *Id.* at 14–19.

[94] *Id.* at 18–21.

[95] *Id.* at 23–24.

[96] *Id.* at 17.

[97] *Id.* at 119.

Table 1
Selected FATF Recommendations Relevant to Internet Gaming Regulators

No.	Recommendation
10	*Customer Due Diligence* • Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names. • Financial institution should be required to undertake customer due diligence measures when, *inter alia*: establishing business relations; carrying out occasional transactions above the applicable designated threshold (US$/€3,000, in the case of Internet casinos); there is a suspicion of money laundering or terrorist financing; or, the financial institution has doubts about the veracity or adequacy of previously-obtained customer identification data. • The principle that financial institutions should conduct customer due diligence should be set out in law. • Customer due diligence measures include the following: (a) identifying the customer and verifying that customer's identity using reliable, independent source documents, data or information; (b) identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner, such that the financial institution is satisfied that it knows who the beneficial owner is; (c) understanding and obtaining information on the purpose and intended nature of the business relationship; and, (d) conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship. • Financial institutions should be required to apply the customer due diligence measures, but should determine the extent of such measures using a risk-based approach. • Financial institutions should be required to verify the identity of the customer and beneficial owner before or during the course of establishing a business relationship or conducting transactions for occasional customers. • Where the financial institution is unable to comply with the applicable customer due diligence requirements, it should be required not to open the account, commence business relations, or perform the transaction, or should be required to terminate the business relationship; and, it should consider making a suspicious transactions report in relation to the customer.
11	*Record-Keeping* • Financial institutions should be required to maintain, for at least five years, all necessary records on transactions to enable them to comply swiftly with information requests from competent authorities. Such records must be sufficient to permit reconstruction of individual transactions (including the amounts and types of currency involved, if any) so as to provide evidence for prosecution of criminal activity. • Financial institutions should be required to keep all records obtained through customer due diligence measures, account files and business correspondence, including the results of any analysis undertaken (*e.g.*, inquiries to establish the background and purpose of complex, unusual large transactions), for at least five years after the business relationship has ended, or after the date of the occasional transaction. • Financial institutions should be required by law to maintain records on transactions and information obtained through customer due diligence measures. • The customer due diligence information and the transaction records should be

	available to domestic competent authorities upon appropriate authority.
12	*Politically Exposed Persons*[98] • Financial institutions should be required, in relation to foreign politically exposed persons ("**PEPs**") (whether as customer or beneficial owner), and in addition to performing normal customer due diligence measures, to: (a) have appropriate risk-management systems to determine whether the customer or the beneficial owner is a PEP; (b) obtain senior management approval for establishing (or continuing, for existing customers) such business relationships; (c) take reasonable measures to establish the source of wealth and source of funds; and, (d) conduct enhanced ongoing monitoring of the business relationship. • Financial institutions should be required to take reasonable measures to determine whether a customer or beneficial owner is a domestic PEP or a person who is or has been entrusted with a prominent function by an international organization. • The requirements for all types of PEP should also apply to family members or close associates of such PEPs.
14	*MVTS* • Countries should take measures to ensure that natural or legal persons that provide MVTS are licensed or registered, and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations. Countries should take action to identify natural or legal persons that carry out MVTS without a license or registration, and to apply appropriate sanctions.
15	*New Technologies* • Countries and financial institutions should identify and assess the money laundering or terrorist financing risks that may arise in relation to: the development of new products and new business practices, including new delivery mechanisms; and, the use of new or developing technologies for both new and pre-existing products. In the case of financial institutions, such a risk assessment should take place prior to the launch of the new products, business practices or the use of new or developing technologies. They should take appropriate measures to manage and mitigate those risks.
17	*Reliance on Third Parties* • Countries may permit financial institutions to rely on third parties to perform elements (a)–(c) of the customer due diligence measures set out in recommendation 10 or to introduce business, provided that the criteria set out below are met. Where such reliance is permitted, the ultimate responsibility for customer due dil-

[98] Politically exposed persons are defined in the 40 Recommendations as follows: "Foreign PEPs are individuals who are or have been entrusted with prominent public functions by a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Domestic PEPs are individuals who are or have been entrusted domestically with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Persons who are or have been entrusted with a prominent function by an international organisation refers to members of senior management, *i.e.* directors, deputy directors and members of the board or equivalent functions. The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories." *Id.*

	igence measures remains with the financial institution relying on the third party. • The criteria that should be met are as follows: (a) a financial institution relying upon a third party should immediately obtain the necessary information concerning elements (a)–(c) of the customer due diligence measures set out in recommendation 10; (b) financial institutions should take adequate steps to satisfy themselves that copies of identification data and other relevant documentation relating to the customer due diligence requirements will be made available from the third party upon request and without delay; (c) the financial institution should satisfy itself that the third party is regulated, supervised or monitored for, and has measures in place for compliance with, customer due diligence and record-keeping requirements in line with recommendations 10 and 11; and, (d) when determining in which countries the third party that meets the conditions can be based, countries should have regard to information available on the level of country risk. • When a financial institution relies on a third party that is part of the same financial group, and: that group applies customer due diligence and record-keeping requirements, in line with recommendations 10, 11, and 12, and programmes against money laundering and terrorist financing, in accordance with recommendation 18; and, where the effective implementation of those customer due diligence and record-keeping requirements and AML/CFT programmes is supervised at a group level by a competent authority, then relevant competent authorities may consider that the financial institution applies measures under (b) and (c), above, through its group programme, and may decide that (d) is not a necessary precondition to reliance when higher country risk is adequately mitigated by the group AML/CFT policies.
18	*Internal Controls and Foreign Branches and Subsidiaries* • Financial institutions should be required to implement programmes against money laundering and terrorist financing. Financial groups should be required to implement groupwide programmes against money laundering and terrorist financing. • Financial institutions should be required to ensure that their foreign branches and majority owned subsidiaries apply AML/CFT measures consistent with the home country requirements.
19	*Higher-Risk Countries* • Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.
20	*Reporting of Suspicious Transactions* • If a financial institution suspects or has reasonable grounds to suspect that funds are the proceeds of a criminal activity, or are related to terrorist financing, it should be required, by law, to report promptly its suspicions to the financial intelligence unit (the "**FIU**").
21	*Tipping-Off and Confidentiality* • Financial institutions and their directors, officers, and employees should be: (a) protected by law from criminal and civil liability for breach of any restriction on disclosure of information imposed by contract or by any legislative, regulatory or administrative provision, if they report their suspicions in good faith to the FIU, even if they did not know precisely what the underlying criminal

	activity was, and regardless of whether illegal activity actually occurred; and, (b) prohibited by law from disclosing ("tipping-off") the fact that a suspicious transaction report or related information is being filed with the FIU.
22	*DNFBPs: Customer Due Diligence* • The customer due diligence and record-keeping requirements set out in recommendations 10, 11, 12, 15, and 17 apply to casinos—including Internet casinos—when customers engage in financial transactions above the US$/€3,000 threshold.
23	*DNFBPs: Other Measures* • The requirements set out in recommendations 18–21 apply to all DNFBPs, subject to certain qualifications that do not apply to Internet casinos.
28	*Regulation and Supervision of DNFBPs* • Casinos—as DNFBPs—should be subject to a comprehensive regulatory and supervisory regime that ensures that they have effectively implemented the necessary AML/CFT measures. At a minimum: (a) they should be licensed; (b) competent authorities should take the necessary legal or regulatory measures to prevent criminals or their associates from holding, or being the beneficial owners of, a significant or controlling interest, holding management functions in, or being operators of, a casino; and, (c) competent authorities should ensure that casinos are effectively supervised for compliance with AML/CFT requirements.

As we shall see, many of the Internet gaming jurisdictions to be canvassed here have requirements that overlap significantly with the 40 Recommendations or expressly appeal to the 40 Recommendations in establishing anti-money laundering policies and procedures.

4.2. Alderney

Alderney is the third-largest of the Channel Islands, located off the French coast of Normandy and approximately 60 miles from England.[99] Alderney is a British Crown Dependency, is self-governing, and is independent of and not subject to the United Kingdom Parliament.[100] The United Kingdom handles the external defence needs and foreign affairs for the Channel Islands, as well as their relationship with the European Union.[101] Alderney does not form part of the EU, but it is inside the customs union.[102]

The key piece of legislation governing Internet gaming conducted from Alderney is the Alderney eGambling Ordinance, 2009 (the "**Alderney Ordinance**").[103] Among other things, the Alderney Ordinance sets out two

[99] John Clitheroe & Richard McMahon, *Alderney*, *in* INTERNET GAMBLING REPORT 531 (10th ed., Mark Balestra, ed., 2007).

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] The Alderney eGambling Ordinance, 2009, *available at*

basic forms of Internet gaming licence that may be obtained: a Category 1 eGambling licence (for business-to-consumer operators) and a Category 2 eGambling licence (for business-to-business operators).[104] The Alderney Gambling Control Commission (the "**AGCC**") is the body charged with granting[105] and revoking licences,[106] promulgating regulations,[107] and overseeing and monitoring the industry's licensees from Alderney.[108] Only Alderney companies may hold Category 1[109] or Category 2 eGambling licences.[110]

The Alderney Ordinance mandates generally that the AGCC is to make regulations providing for the way in which an eGambling licensee (of whatever class) is "obliged to take steps to comply with applicable international measures in respect of money laundering and terrorist financing."[111] These components, among others, are in the Alderney eGambling Regulations 2009 (the "**Alderney Regulations**"). Before turning to Schedule 16 (the money laundering and terrorist financing provisions) thereof, we shall briefly summarize the suitability requirements for licensure under licence Categories 1 and 2.

The procedure for applying for a Category 1 or 2 eGambling Licence is set out in sections 16 and 17 of the Alderney Regulations. The Alderney Regulations also set out criteria against which the applicant is to be considered.[112] While these appear to be comprehensive, the application fee to cover processing and—crucially—investigation of the applicant (£10,000)[113] appears low compared with other leading jurisdictions (*e.g.*, Nevada). *Quaere* whether a proper and complete investigation of suitability of an enterprise can be done for this amount. Note, however, that the AGCC may require the deposit of further investigation and other costs with it from the applicant.[114] The required forms for eGambling licence applicants in Schedule 1

---

http://www.gamblingcontrol.org/userfiles/file/Alderney%20eGambling%20Ordinance%202009%20final%20version.pdf.

[104] *See id.* at §4(1). *See also* Alderney eGambling Regulations 2009, §§ 3–6, a*vailable at* http://www.gamblingcontrol.org/userfiles/file/2009_regs_consolidated_with_2010%20%201%20%202%20and%202011%20amendments.pdf. Note that other forms of licensure and certifications are also available, *e.g.*, Temporary eGambling licences and key individual certificates.

[105] The Alderney eGambling Ordinance, 2009, *supra* note 103, §§ 4, 5, and 7.

[106] *Id.* § 12.

[107] *See, e.g. id.* §§ 4(2) and 4(3).

[108] *See, e.g. id.* §§ 14, 15, and 21.

[109] Alderney eGambling Regulations 2009, *supra* note 104, § 3(3).

[110] *Id.* § 5(4).

[111] The Alderney eGambling Ordinance, 2009, *supra* note 103, § 22(2)(e).

[112] Alderney eGambling Regulations 2009, *supra* note 104, § 21.

[113] *Id.* Sched. 21.

[114] *Id.* § 27.

to the Alderney Regulations are not comprehensive. For example, only "known" shareholders of the applicant or the applicant's parent holding 3% of the respective issued and outstanding share capital are inquired about (as opposed to listing all registered shareholders). Audited accounts are requested, but there are no express questions about previous liquidation, insolvency, or bankruptcy proceedings. (But note that section 21 has "the applicant's current financial position and financial background" as a criterion against which the applicant is assessed for licensure.[115])

As to key individuals, again the initial investigatory and processing fee (£1,000)[116] seems low. However, the criteria for assessment are broad[117] and the disclosure[118] seems designed to elicit more information than in the case of eGambling licence applicants. Overall, it is unclear how well the Alderney rules and procedures function in terms of admitting only suitable organizations and individuals.

After suitability, the key components of the anti-money laundering protocols contained in the Alderney Regulations are in Schedule 16. Section 1 in Schedule 16 sets out completion of a business risk assessment as a precondition for approval of the eGambling licensee's internal control system. The concept of risk—consistent with the FATF's required risk-based approach—runs throughout the Schedule.[119]

Category 1 (business-to-consumer) licensees are to undertake customer due diligence measures: subject to section 4 of Schedule 16,[120] before registering a customer;[121] immediately after a registered customer makes a deposit equal to or greater than €3,000—reflecting the FATF threshold—or makes a deposit bringing the total deposits made by her in any 24 hour period equal to or greater than €3,000;[122] when it reasonably knows or suspects that a person is engaged in money laundering or terrorist financing;[123] or, when it doubts the truth or sufficiency of any information previously obtained for purposes of customer identification or verification.[124] Enhanced customer due diligence is to take place, for instance, where a Category 1 eGambling licensee does business with a customer who is a PEP[125] or a customer "es-

---

[115] *Id.* § 21.

[116] *Id.* Sched. 21.

[117] *Id.* § 142.

[118] *Id.* Sched. 9.

[119] *See, e.g.* "high risk" customers referred to in *id.* Sched. 16, § 6(1)(a).

[120] Allowing identification and verification procedures after registration under certain circumstances.

[121] Alderney eGambling Regulations 2009, *supra* note 104, Sched. 16, § 2(a).

[122] *Id.* Sched. 16, § 2(b).

[123] *Id.* Sched. 16, § 2(c).

[124] *Id.* Sched. 16, § 2(d).

[125] *Id.* Sched. 16, § 3(1)(a).

tablished or situated" in a country that does not apply or insufficiently applies the 40 Recommendations.[126]

With specific respect to customer due diligence and identification and verification procedures, the Alderney Regulations indicate that a Category 1 eGambling licensee is required to undertake an individual risk assessment of each customer in accordance with the licensee's internal control systems.[127] Alderney's anti-money laundering guidance notes (the "**Alderney Guidance**") suggest that the personal information to be collected by a Category 1 eGambling licensee "will include … unique identifiers contained within official documents such as driving licences, passports or identity cards."[128] However, the Alderney Guidance fundamentally leaves things open for the Class 1 operator, providing that it "must determine, in accordance with the risk based approach set out in its Business Risk Assessment the extent of the identification and verification information to ask for, what to verify and how this information is to be verified in order to be satisfied as to the identity of its customer, beneficial owner or underlying principal."[129] This more flexible approach appeared to be in effect when the author registered and deposited a small amount of funds with an Alderney Category 1 eGambling licensee. No details of official government documents were requested or provided; only name, address, country of residence, date of birth, country of residence, and credit card information were given.[130]

One example from the Alderney Guidance may indicate a somewhat mechanical approach to deposit-based verification. The example posits a customer making a deposit of €2,950 and then subsequently making a further deposit of €100 23 hours later.[131] In such a case, customer due diligence is to be performed. By contrast, a customer depositing €2,950 and a further €100 23 hours thereafter would not automatically trigger customer due diligence, "however the licensee may consider the transactions to be linked for other reasons, which would trigger CDD [customer due diligence]."[132] Also

---

[126] *Id.* Sched. 16, § 3(1)(b).

[127] *Id.* § 227(2).

[128] Alderney Gambling Control Commission, The Prevention of Money Laundering and Combating the Financing of Terrorism—Guidance for the eGambling Industry Based in Alderney 24, *available at* http://www.gamblingcontrol.org/userfiles/file/AML%20and%20CFT%20guidance%202010.pdf%20LdeL.pdf.

[129] *Id.* at 23.

[130] Note that this may be in accordance with, among other things, the terms of subsection 227(4) of the Alderney Regulations.

[131] Alderney Gambling Control Commission, The Prevention of Money Laundering and Combating the Financing of Terrorism—Guidance for the eGambling Industry Based in Alderney, *supra* note 128, at 28.

[132] *Id.*

note that such transactions could be seen as higher risk under a risk-based approach, especially if repeated.

If a Category 1 eGambling licensee cannot comply with the regular customer due diligence procedures, the licensee is to not register the customer[133] or must terminate the customer relationship,[134] as may be, and consider whether disclosure is required[135] pursuant to the Disclosure (Bailiwick of Guernsey) Law, 2007[136] (the "**Disclosure Law**") or the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002[137] (the "**Terrorism Law**"). There are also general provisions in the Alderney Regulations setting out that the Category 1 licensee must perform ongoing and effective monitoring of any existing customer relationship,[138] including scrutinizing complex[139] or large and unusual transactions[140] or unusual patterns of transactions.[141] (Category 2 eGambling licensees are addressed separately.[142])

Reporting suspicious activities is covered in section 7 of Schedule 16, with reference both to Part I of the Disclosure Law, which covers both financial services and non-financial services businesses, and to section 12 of the Terrorism Law. Both Category 1 and Category 2 licensees are duty-bound to follow the reporting strictures in Schedule 16. The Alderney Regulations set out requirements for both Category 1 and Category 2 eGambling licensees to appoint a money laundering reporting officer, as well as that officer's responsibilities.[143] There are also provisions for ensuring that "relevant employees" receive training in, *inter alia*, the Alderney Ordinance and the Alderney Regulations;[144] internal procedures and controls to prevent money laundering;[145] the identity and responsibility of the money laundering reporting officer;[146] and, the detection of unusual or suspicious transactions.[147] Tipping-off is addressed in section 4 of the Disclosure Law.

---

[133] Alderney eGambling Regulations 2009, *supra* note 104, Sched. 16, § 5(a).

[134] *Id.* Sched. 16, § 5(b).

[135] *Id.* Sched. 16, § 5(c).

[136] The Disclosure (Bailiwick of Guernsey) Law, 2007, *available at* http://www.gamblingcontrol.org/userfiles/file/60.pdf.

[137] The Terrorism and Crime (Bailiwick of Guernsey) Law, 2002, *available at* http://www.gamblingcontrol.org/userfiles/file/Terrorism_and_Crime_(Bailiwick_of_Guernsey)_Law,_2002_(Consolidated%202010.pdf.

[138] Alderney eGambling Regulations 2009, *supra* note 104, Sched. 16, § 6(1).

[139] *Id.* Sched. 16, § 6(1)(c)(i).

[140] *Id.* Sched. 16, § 6(1)(c)(ii).

[141] *Id.* Sched. 16, § 6(1)(c)(iii).

[142] *Id.* Sched. 16, § 6(1A).

[143] *Id.* Sched. 16, § 7(1).

[144] *Id.* Sched. 16, § 8(1)(b)(i).

[145] *Id.* Sched. 16, § 8(1)(b)(iv).

[146] *Id.* Sched. 16, § 8(1)(b)(v).

[147] *Id.* Sched. 16, § 8(1)(b)(vi).

On record-keeping, the rules generally set out five year retention periods for both Category 1 and 2 licensees, consistent with the 40 Recommendations. For example, transaction documents or copies are to be kept for five years, starting from the date that the transaction and any related transaction(s) were completed.[148] Customer due diligence information is to be retained for five years starting from the date the person ceased to be a customer.[149] The Alderney Regulations also make provisions for retaining copies of documents when required to be produced pursuant to court order.[150] The AGCC's Technical Standards and Guidelines for Internal Control Systems and Internet Gambling Systems specify that all "gambling information" (inclusive of customer account and session information) should be retained by a licensee for six years.[151]

Note that there are sanctions imposed against different actors by Guernsey, which therefore includes Alderney, having the effect of prohibiting certain transactions (including gaming transactions) with or involving those persons.[152]

On banking and payment processing methods and providers for Category 1 licensees, the Alderney Guidance is somewhat helpful in addressing risks:

> The risks of money laundering can be reduced by ensuring that deposits originate from an account with a recognised financial body in the name of the customer. In addition, the risk of money laundering can be further reduced by ensuring that withdrawals are made to the same credit/debit card or account as the original deposit came from. Those Category 1 eGambling licensees who make use of alternative deposit or withdrawal methods (such as third party payment processors) should be aware that this increases the risk of money laundering and their business risk assessments must address this factor.[153]

As we shall see, more specific guidance in this particular area may be salutary.

---

[148] *Id.* Sched. 16, § 9(1)(a).

[149] *Id.* Sched. 16, § 9(1)(b).

[150] *Id.* Sched. 16, § 9(2).

[151] Alderney Gambling Control Commission, Technical Standards and Guidelines for Internal Control Systems and Internet Gambling Systems 106–107 (2010), *available at*
http://www.gamblingcontrol.org/userfiles/file/ICSG%20Version%203_1%20DRAFT%20v2_0_b.pdf.

[152] *See, e.g.* Guernsey Financial Investigation Unit, Guernsey Renews Sanction Regime Al-Qaida and Taliban, *available at*
http://guernseyfiu.gov.gg/article/6481/Guernsey-Renews-Sanction-Regime-Al-Qaida-and-Taliban.

[153] Alderney Gambling Control Commission, The Prevention of Money Laundering and Combating the Financing of Terrorism—Guidance for the eGambling Industry Based in Alderney, *supra* note 128, at 13.

Fortunately, it is possible to obtain an objective third party view of how the AGCC is doing at deterring money laundering by reading the IMF's most recent detailed assessment report for Guernsey from January 2011. While the IMF agrees that the AGCC's supervision of interactive gaming operators is extensive,[154] it also notes some areas of concern. One worry is the lack of consistent police record checks on individuals in the licensing process, creating "a risk that the industry may be infiltrated by criminals."[155] Another is with respect to requesting reimbursement through a different payment mechanism than that used by a customer to deposit or through payment mechanisms that allow transactions between players. The AGCC requires controls on such payments, but they are at the AGCC's discretion; they are not prohibited under the Alderney Ordinance or the Alderney Regulations. The IMF's "assessment team did not find wide use of these mechanisms during the on-site visit but the vulnerabilities with respect to the payment mechanism is [*sic*] still present in absence of legislative or regulatory prohibitions."[156] The IMF also remarked on what it called "insufficient" suspicious transaction reporting by gaming operators given the risk level and the transactions volume conducted by the industry.[157]

4.3. Isle of Man

The Isle of Man is another Crown Dependency,[158] this one situated in the Irish Sea between Britain and Ireland.[159] As with Alderney, the UK Parliament does not legislate in respect of the Isle of Man's internal affairs, but is responsible for its defence and foreign affairs.[160] The Isle of Man is not a member of the EU, but it is inside the customs union.[161]

The starting point for the Isle of Man's Internet gaming and betting regulatory regime is the Online Gambling Regulation Act 2001 (the "**Isle of Man Act**").[162] This sets out the Isle of Man Gambling Supervision Commission's (the "**GSC's**") authority to issue licences to conduct online gam-

---

[154] International Monetary Fund, Guernsey: Detailed Assessment Report on Anti-Money Laundering and Combating the Financing of Terrorism 275 (2011), *available at* http://www.imf.org/external/pubs/ft/scr/2011/cr1112.pdf.

[155] *Id.* at 15.

[156] *Id.* at 231.

[157] *Id.* at 266.

[158] Claire Milne, *E-Gaming in the Isle of Man: A Primer*, 14 Gam. L. Rev. & Econ. 371 (2010).

[159] Miles Benham, *The Isle of Man*, *in* Internet Gambling Report 507 (10th ed., Mark Balestra, ed., 2007).

[160] Milne, *supra* note 158.

[161] *Id.*

[162] Online Gambling Regulation Act 2001, ch. 10 (IOM), *available at* http://www.gov.im/lib/docs/gambling/Regulations/onlinegamblingregulationact2001.pdf.

bling,[163] to set the conditions of licensure,[164] and to cancel or suspend a licence.[165] The two key classes of licence are the standard licence (for business-to-consumer operators)[166] and the network services licence (for business-to-business operators).[167] Both licences require a Manx corporation to be the licensee.[168]

The Isle of Man Act establishes that the GSC cannot grant any licence unless it is satisfied that the licensee is under the control of[169]—and that its activities are under the management of—persons of integrity.[170] The application fee for a licence is £5,000,[171] which appears low for normal investigatory costs. Presumably further funds can be requisitioned from applicants to defray additional investigatory costs if those need to be incurred. There is no fee in respect of key officials, which seems inadequate. The required forms for licence applicants are not onerous. For example, only shareholders holding more than five per cent of the issued share capital of the applicant company must disclose their names and shareholdings and complete personal declaration forms. Audited accounts are requested but, here again, there are no express inquiries about previous insolvencies or certain other events. Separate disclosure is required of a parent corporation (for example), but the same five per cent rule with respect to disclosure of shareholders of the parent also appears to be in effect. The personal declaration forms are not robust. For instance, disclosure only of a key individual's "main personal banking account" is required. No particulars with respect to other assets or any liabilities—save and except for a yes–no check box with respect to being in default of credit cards, mortgages, or other financial liabilities—are solicited.

All licensees are subsumed under the term "licence holder" in the Proceeds of Crime (Money Laundering—Online Gambling) Code 2010 (the

---

[163] *Id.* § 4(1).

[164] *Id.* § 6.

[165] *Id.* § 13.

[166] *See generally* Online Gambling (Licence Fees) Regulations 2009, S.D. 257/09 (IOM), *available at*
http://www.gov.im/lib/docs/gambling/Regulations/onlinegamblinglicencefeesregul.pdf.

[167] *See generally* Online Gambling Regulations (Amendment) (Network Services) Regulations 2011, S.D. 003/11, *available at*
http://www.gov.im/lib/docs/gambling//networkregulations.pdf.

[168] Online Gambling Regulation Act 2001, ch. 10 (IOM), *supra* note 162, § 4(1).

[169] *Id.* § 4(2)(a).

[170] *Id.* § 4(2)(c).

[171] Isle of Man Gambling Supervision Commission, Guidance for On-line Gambling 13 (2011), *available at* http://www.gov.im/gambling/applications.xml (follow "Guidance Notes for making an Online Gambling application" hyperlink).

"**Isle of Man Code**"),[172] which sets out procedures and rules that all licence holders in the Isle of Man must follow.[173] The Isle of Man Code mandates that a risk assessment be undertaken in order to determine the measures to be taken when carrying out player or business participant due diligence or enhanced due diligence.[174] The risk assessment is to estimate the risk of money laundering having regard to several factors.[175] Moreover, the Isle of Man anti-money laundering guidance notes (the "**Isle of Man Guidance**") advocate a risk-based approach to all aspects of the Isle of Man Code.[176] The Isle of Man Code prohibits the acceptance of cash by a licence holder from any customer or business participant—and prohibits acceptance of cash on its behalf by any third party—in relation to Internet gaming.[177] It also expressly prohibits the maintenance of accounts by licence holders that are anonymous[178] or in fictitious names,[179] in line with the 40 Recommendations.

The customer due diligence requirements in the Isle of Man appear to be somewhat less confusing than the comparable Alderney requirements. When a player wants to establish an account with a B2C licence holder, the licence holder is to "require the prospective participant to provide satisfactory information as to his identity … as soon as reasonably practicable after contact is first made between them."[180] What this means is that B2C licence holders in the Isle of Man must obtain the full name, residential address, date of birth, place of birth, and nationality of each player at registration.[181] This is all input by the player. There is no requirement to, for example, tender copies or numbers of government documents at this stage.

In the B2C model, further identification requirements are engaged when "a qualifying payment is to be made to a participant [player] in relation to

---

[172] Proceeds of Crime (Money Laundering—Online Gambling) Code 2010, S.D. 509/10 (IOM), *available at* http://www.gov.im/lib/docs/gambling//amlgamblingcode2010final.pdf.

[173] *Id.* § 3.

[174] *Id.* § 5(1).

[175] *Id.* § 5(2).

[176] Isle of Man Gambling Supervision Commission, Online Gambling Guidance Notes for the Prevention of Money Laundering and Countering of Terrorist Financing 12 (2011), *available at* http://www.gov.im/gambling/licensing/ (follow "Guidance Notes for the Prevention of Money Laundering and Countering of Terrorist Financing" hyperlink).

[177] Proceeds of Crime (Money Laundering—Online Gambling) Code 2010, S.D. 509/10 (IOM), *supra* note 172, § 3(2).

[178] *Id.* § 4(1)(a).

[179] *Id.* § 4(1)(b).

[180] *Id.* § 6(1).

[181] Isle of Man Gambling Supervision Commission, Online Gambling Guidance Notes for the Prevention of Money Laundering and Countering of Terrorist Financing, *supra* note 176, at 30; Brennan Interview, *supra* note 10.

online gambling."[182] Licence holders are to establish, maintain, and operate procedures requiring a customer to produce satisfactory evidence of her identify prior to making the qualifying payment.[183] A qualifying payment is a payment that exceeds €3,000,[184] or a payment in respect of which, when taken with all other payments made to the customer within the thirty days immediately preceding the date on which the payment is to be made, the aggregate amount exceeds €3,000.[185] This is consistent with the €3,000 threshold set for casinos by the 40 Recommendations. The documentation that is required here, *i.e.*, that is to be "obtained and retained"[186] by the licence holder, is generally some form of government-issued identification.[187]

Evidence of identity for business participants—including suppliers and business customers in a B2B model—is addressed in section 8 of the Isle of Man Code. Enhanced due diligence in respect of certain players, suppliers, and business customers is also covered in the Isle of Man Code; these measures apply to, among others, PEPs[188] and to persons located in a country that the licence holder has reason to believe does not apply or insufficiently applies the 40 Recommendations.[189] Sundry ongoing monitoring steps are also required to be taken by licence holders.[190]

According to the GSC's Chief Executive, these are the minimum thresholds set out by law and they are in line with the 40 Recommendations. However, he adds that, in applying a risk-based approach, many of the Isle of Man's licence holders will elect to implement further due diligence controls and identification procedures at earlier transactional stages and where increased risk is perceived.[191] In fact, this is the case with Paddy Power, a major interactive gaming and betting operator in the Isle of Man.[192] At Paddy Power, consistent with section 6 in the Isle of Man Code, certain information is obtained at the point of registration, *i.e.*, full name, residential address, date of birth, place of birth, and nationality. At the deposit stage,

---

[182] Proceeds of Crime (Money Laundering—Online Gambling) Code 2010, S.D. 509/10 (IOM), *supra* note 172, § 7(1).

[183] *Id.* § 7(2).

[184] *Id.* § 7(3)(a).

[185] *Id.* § 7(3)(b).

[186] Isle of Man Gambling Supervision Commission, Online Gambling Guidance Notes for the Prevention of Money Laundering and Countering of Terrorist Financing, *supra* note 176, at 31.

[187] *Id.*; Brennan Interview, *supra* note 9.

[188] Proceeds of Crime (Money Laundering—Online Gambling) Code 2010, S.D. 509/10 (IOM), *supra* note 172, § 9(2)(a).

[189] *Id.* § 9(2)(b).

[190] *Id.* § 10.

[191] Brennan Interview, *supra* note 10.

[192] The licensee in the Isle of Man is Paddy Power Holdings Limited. Paddy Power plc is a publicly-traded corporation on the Irish and London stock exchanges.

the bulk of Paddy Power's risk assessment protocols are engaged.[193] Paddy Power has a dedicated customer security team and runs constant reports based upon deposits reaching certain thresholds and its customers fitting various risk profiles.[194] For example, if a new customer deposits using a credit card in the ordinary course, the threshold for automatic review would be higher than if the deposit method were by means of an e-wallet or a prepaid voucher.[195] (Note that this review would apply irrespective of the €3,000 threshold set out in paragraph 7(3)(b) of the Isle of Man Code, which only applies to withdrawals.) There are also reports based on, *inter alia*, frequency and patterns of play, payment activities, and deposit and withdrawal methods.[196] The thresholds and risk profiles in these sundry reports are dynamic and subject to constant revision and refinement.[197]

When a Paddy Power customer appears on one or more reports, the enterprise will seek to validate that customer using a suite of tools and inquiries. This ranges from inquiries placed against external proprietary databases of information through to direct questioning of the customer to determine the source of funds.[198] If the sources of funds cannot be ascertained to Paddy Power's satisfaction, a suspicious transaction report is made to the relevant Isle of Man authority.[199]

According to Paddy Power's compliance manager, who is also the enterprise's deputy money laundering reporting officer pursuant to applicable Isle of Man law, the vast majority of their B2C customers are electronically verified in some manner within a short period after their initial deposit to their online interactive gaming account.[200] This may indicate that there are an extensive number of sorts through which all customers pass and are vetted.

The Isle of Man Code states that records of all transactions with players and business participants are to be generated and kept by the licence holder sufficient to demonstrate that money laundering regulations have been complied with.[201] These records must be kept for a period of at least six years, as applicable, from the date the player or business participant formal-

---

[193] Interview with Robert Reddin, Compliance Manager, Paddy Power plc (Feb. 10, 2012) [hereinafter Reddin Interview].

[194] *Id.*

[195] *Id.*

[196] *Id.*

[197] *Id.*

[198] *Id.*

[199] *Id.*

[200] *Id.*

[201] Proceeds of Crime (Money Laundering—Online Gambling) Code 2010, S.D. 509/10 (IOM), *supra* note 172, § 12.

ly ceased to be a player or business participant;[202] or, the date of the last transaction carried out by the player or business participant.[203] Note this is longer than the five year minimum prescribed by the 40 Recommendations. The GSC takes the view that all items required to be tracked, recorded, and available for access by appropriate authorities in the Online Gambling (Systems Verification) (No. 2) Regulations 2007 (including detailed records on all gaming sessions on the licence holder's site) are also subject to this minimum six-year retention rule.[204]

As regards the reporting of suspicious transactions, a money laundering reporting officer must be appointed by each licence holder.[205] This officer is the lynchpin of the licence holder's internal and external reporting procedures. The money laundering reporting officer is to be sufficiently senior within the organization[206] (or must have sufficient experience and authority, if not within the organization)[207] and must have a right of direct access to the directors or managing board of the licence holder.[208] Among other functions, the money laundering reporting officer effectively initiates the disclosure of any applicable suspicious transaction reports to the Isle of Man Financial Crime Unit.[209] Staff screening and training by a licence holder is addressed in sections 17 and 18, respectively, of the Isle of Man Code.

Interestingly, in a reflection of the FATF's recommendation 15 (new technologies), the Isle of Man's rules provide that a licence holder must maintain appropriate procedures and controls to prevent "the misuse of technological developments for the purpose of money laundering or the financing of terrorism."[210] This is a clear call for constant vigilance about the exploitation of new technology. Such a provision is also consonant with the risk-based approach adopted by the Isle of Man.

Tipping-off is covered in the Isle of Man Guidance. The offence itself is described in subsection 6.8.4(1)–(3), while the penalties associated with the offence are described in subsection 6.8.4(4). There is a current list of sanc-

---

[202] *Id.* § 13(1)(a).

[203] *Id.* § 13(1)(b).

[204] Brennan Interview, *supra* note 10.

[205] Proceeds of Crime (Money Laundering—Online Gambling) Code 2010, S.D. 509/10 (IOM), *supra* note 172, § 16(1).

[206] *Id.* § 16(2)(a).

[207] *Id.* § 16(2)(b).

[208] *Id.* § 16(2)(c).

[209] *Id.* § 16(3)(f). The money laundering reporting officer's role is expanded upon in Isle of Man Gambling Supervision Commission, Online Gambling Guidance Notes for the Prevention of Money Laundering and Countering of Terrorist Financing, *supra* note 176, at 10–12.

[210] Proceeds of Crime (Money Laundering—Online Gambling) Code 2010, S.D. 509/10 (IOM), *supra* note 172, § 19.

tions imposed by the Isle of Man as against selected territories and institutions.[211]

With respect to banking and payment processing, interviews with the GSC and with an operator regulated in the Isle of Man were insightful. The regulator acknowledged that, in an ideal world, the Isle of Man's operators would only accept credit and debit cards for payments from major providers.[212] However, the GSC again favours a risk-based approach as advocated by the 40 Recommendations. Its licence holders have a requirement pursuant to applicable Isle of Man law to understand with whom they're doing business. This extends to banks' and payment intermediaries' internal controls and procedures to vet their own users and customers.[213] On the operator side, Paddy Power, for example, takes a risk-based approach but tries at all times to deal with "cleaner" operators: the larger organizations that have a positive market reputation and are heavily regulated.[214]

The most recent detailed assessment report compiled by the IMF for the Isle of Man is from 2009. The GSC received generally positive marks in this assessment. However, the IMF did note that additional resources—particularly staffing resources and specialist skills—would need to be allocated to the GSC to keep pace with its workload and the growth of the Internet gaming sector in the Isle of Man.[215]

4.4. Kahnawá:ke

The Mohawk Territory of Kahnawá:ke is an aboriginal community of approximately 8,000 people located 20 minutes from Montreal, Canada.[216] The entire territory occupies approximately 20 square miles.[217] The Mohawk Council of Kahnawá:ke (the "**Mohawk Council**") is the governing body in and for the territory and is composed of eleven chiefs and one grand chief, all of whom are popularly elected by the community.[218] Kahnawá:ke has consistently and historically asserted sovereignty over its affairs and territory. Kahnawá:ke has its own police force, court, schools, hospital, fire services, and social services.[219]

---

[211] Isle of Man Treasury Department, Sanctions and Export Control in the Isle of Man, *available at* http://www.gov.im/treasury/customs/sanctions.xml.

[212] Brennan Interview, *supra* note 10.

[213] *Id.*

[214] Reddin Interview, *supra* note 193.

[215] IMF Isle of Man Report, *supra* note 70, at 20 and 207–208.

[216] Murray Marshall, *Kahnawake*, *in* Internet Gambling Report 321 (5th ed., Mark Balestra, ed., 2002).

[217] *Id.*

[218] *Id.* at 322.

[219] *Id.*

The Kahnawá:ke Gaming Commission (the "**KGC**") was established by the Kahnawá:ke Gaming Law, enacted by the Mohawk Council in 1996.[220] The KGC's basic mandate is to regulate and control gaming taking place within or from Kahnawá:ke.[221] Assessing the suitability of interactive gaming licence holders and implementing money laundering controls is done under the rubric of the Regulations Concerning Interactive Gaming (the "**KGC Regulations**"),[222] originally promulgated by the KGC in 1999.

The KGC Regulations set out two types of licence: the Interactive Gaming Licence (only one of which has been issued by the KGC, to Mohawk Internet Technologies, a band-empowered entity wholly owned by the Mohawk Council); and, the Client Provider Authorization (the "**CPA**"). The CPA is the licence that is obtained by private Internet gaming operators seeking to be "licensed" by Kahnawá:ke. The holder of a CPA may conduct interactive gaming from Kahnawá:ke, "but only from the co-location facility that is owned and operated by the holder of a valid Interactive Gaming Licence."[223]

To apply for a CPA, copious information must be provided and prescribed forms completed.[224] The data solicited in this process appears to be extensive and useful for determining suitability. The cost for applying is US$25,000, which includes the estimated cost of the KGC conducting due diligence on the applicant and any individuals that have provided personal information forms further to that application.[225] The application cost for each proposed key person licence is US$5,000.[226]

What is much more interesting to an assessment of anti-money laundering controls in Kahnawá:ke than the suitability vetting process or its cost is the absence of many money laundering-specific rules and procedures in the KGC Regulations. The bulk of the money laundering provisions are essentially farmed out by means of section 168, which provides as follows: "Authorized Client Providers will comply with the recommendations of the Financial Action Task Force ("FATF") as they pertain to gaming establishments."[227] In other words, the 40 Recommendations—at least as they apply to Internet casinos—are imported wholesale into the KGC Regulations. Presumably a violation of any of the 40 Recommendations is therefore a violation of the KGC Regulations, as well. Because of the breadth of the 40

---

[220] *Id.*

[221] *Id.*

[222] Regulations Concerning Interactive Gaming (1999) (Kahnawá:ke), *available at* http://gamingcommission.ca/docs/RegulationsConcerningInteractiveGaming.pdf.

[223] *Id.* § 34.

[224] *Id.* §§ 35(a)–35(f).

[225] *Id.* § 35(g).

[226] *Id.* § 35(h).

[227] *Id.* § 168.

Recommendations and how many other regimes seek to mimic or incorporate their terms in any event, this may not be such a bad idea.

However, there are difficulties with such an approach, both in principle and in practice. While the 40 Recommendations are continually being revised and updated, there appears not to have been a great deal of resources devoted specifically to Internet gaming and betting by the FATF. The 40 Recommendations and the RBA Guidance for Casinos include Internet gaming considerations. However, it may be that full-time online interactive gaming regulators are in a better position than the FATF to take the 40 Recommendations and layer on specific additional provisions that benefit the sector and potentially reduce money laundering.

In addition, certain provisions of the 40 Recommendations suggest an ongoing monitoring role by regulators. For example, recommendation 28 provides that competent authorities, which would include gaming regulators, should ensure that casinos are effectively supervised for compliance with anti-money laundering requirements. In this context, it seems odd for the KGC Regulations only to mandate CPA-holder compliance with the 40 Recommendations; there are continuing obligations under the 40 Recommendations with which the KGC is also supposed to comply.[228]

More fundamentally, however, this offloading onto the FATF by the KGC risks diluting the latter's responsibility as a regulator. The essence of proper regulation is robust and properly resourced enforcement of international norms and standards as well as formulation and monitoring of local requirements. By foregoing the creation of detailed local rules, the KGC may be letting go of some of its responsibilities to its stakeholders. The KGC may thereby be making itself less responsive and, ultimately, less relevant as a regulatory body.

It might be easier to support this approach in practice—if not conceptually—if the specific provisions that are in the KGC Regulations did not seem incomplete. Section 163 states that the KGC "will establish specific rules and procedures for Authorized Client Providers for the purpose of anticipating and preventing suspicious activities whereby monies obtained by illegal means are used for the purpose of interactive gaming."[229] However, no such specific rules and procedures appear to be available from the KGC. Another provision establishes that CPA-holders are required to file suspicious activity reports with the KGC under certain conditions, in a

[228] Perhaps not too much should be made of this point. If asked, the KGC might state that its obligation to comply with the 40 Recommendations is well understood and should be taken for granted.

[229] Regulations Concerning Interactive Gaming (1999) (Kahnawá:ke), *supra* note 222, § 163.

form to be provided by the KGC;[230] no forms have yet been prescribed by the KGC for this purpose.

Some other aspects of the KGC Regulations may raise questions. For instance, they set out that the KGC will cooperate and, "when appropriate, provide information concerning actual or potential money-laundering activities of which it becomes aware, to the Kahnawake Peacekeepers and/or such other domestic or international agency or agencies that are appropriate."[231] It is unclear whether such other agencies would include Canada's FIU (referred to in recommendation 20 of the 40 Recommendations), the Financial Transactions and Reports Analysis Centre of Canada ("**FinTRAC**"). This point is the corollary of the FATF's concern about a lack of anti-money laundering regulations in Kahnawá:ke, addressed below. Also, the threshold triggering a suspicious activity report (US$5,000)[232] and the prohibitions on withdrawals in excess of US$10,000 (absent identification)[233] seem to be incongruent with the US$/€3,000 threshold set out in the 40 Recommendations.

The matter of a corporation not needing to be locally formed to obtain a CPA is another interesting item. The KGC Regulations set out no such local corporation requirement, unlike Alderney and the Isle of Man. As we shall see, it may be preferable and a best practice for a corporation that is licensed and regulated by gaming authorities to be set up in the licensing jurisdiction, but perhaps it need not be mandatory. There might be other ways of regulators controlling a licensee, through effective oversight of its technology hosting, the presence of a licensee's books and records in the jurisdiction, having a local office and presence, and any number of other nexus requirements.

Finally, this section would be incomplete without mentioning the FATF's concerns about Kahnawá:ke set out in its latest mutual evaluation report on Canada from February 2008.[234] In the mutual evaluation, the FATF describes the activities and regime set out by the Mohawks in regulating Internet gaming and betting and states that the KGC Regulations "were designed to ensure that all interactive gaming and gaming related activities … satisfy three basic principles: (1) that only suitable persons and entities are permitted to operate within Kahnawake; (2) that the games offered are fair to the player; and (3) that winners are paid."[235]

---

[230] *Id.* § 165.

[231] Id. § 169.

[232] Id. § 165.

[233] Id. § 167(a).

[234] Financial Action Task Force, Third Mutual Evaluation on Anti-Money Laundering and Combating the Financing of Terrorism—Canada (2008), *available at* http://www.fatf-gafi.org/dataoecd/5/3/40323928.pdf.

[235] *Id.* at 231.

However, the FATF expresses serious concerns about Kahnawá:ke from a money laundering perspective, as follows:

> [T]hese activities [the regulation of Internet gaming and betting] are not subject to AML/CFT regulations and Canada's federal and provincial governments are faced with substantial challenges in determining the appropriate course of action to be taken concerning Internet gambling. The industry has grown rapidly and huge revenues are generated. Canada must either enforce its prohibition effectively or introduce comprehensive AML/CFT regulation for the industry.[236]

The statement that regulation by Kahnawá:ke is simply "not subject" to anti-money laundering regulations might be pitching the case too high. As discussed, some anti-money laundering protocols are present in the KGC Regulations. The issue is whether they are complete and appropriate to the responsibilities faced by a tier one regulator. For example, the interaction between Kahnawá:ke and FinTRAC in the context of the KGC Regulations and the 40 Recommendations has been highlighted as an area lacking clarity.

4.5. Malta

Malta is an interesting jurisdiction for its location and the interplay of its anti-money laundering rules with its Internet gaming and betting regulatory regime. Malta is an archipelago near the centre of the Mediterranean Sea, strategically positioned between Sicily and North Africa. Malta is a full member of the EU, a member of the Schengen area, and a member of the euro zone.[237]

Internet gaming in Malta and its licensure is governed primarily by the Lotteries and Other Games Act (the "**LOGA**").[238] Section 9 of the LOGA establishes the Lotteries and Gaming Authority (the "**LGA**"), which is charged with, among other things, inquiring into the suitability of all licensees under the LOGA,[239] ensuring that all gaming is kept free from criminal activity,[240] and advising the Maltese Minister of Finance on the making of applicable regulations.[241] The main regulations in respect of online gaming

---

[236] *Id.*

[237] European Union, Malta, *available at* http://europa.eu/about-eu/countries/member-countries/malta/index_en.htm.

[238] Lotteries and Other Games Act (Malta), *available at* http://www.lga.org.mt/lga/content.aspx?id=87374 (follow "Lotteries and Other Games Act, 2001" hyperlink).

[239] *Id.* § 11(c).

[240] *Id.* § 11(e).

[241] *Id.* § 11(k).

and betting promulgated under the LOGA are the Remote Gaming Regulations (the "**Malta Regulations**").[242]

The Malta Regulations provide for the issuance,[243] suspension, and cancellation[244] of remote gaming licences to carry on various Internet gaming and betting operations. The initial grant is subject to a "fit and proper" determination of those persons involved in the applicant corporation pursuant to subsection 8(2) of the Malta Regulations. Note that, as with Alderney and the Isle of Man, an applicant for a remote gaming licence must be a company incorporated pursuant to the Malta Companies Act.[245] The Malta Regulations provide for four classes of gaming licence, which licences encompass everything from business-to-consumer gaming and betting exchanges to business-to-business network models.[246] At least one "key official" must be appointed by each gaming or betting licensee,[247] who must personally supervise the operations of the licensee of which she is a key official[248] and ensure that the licensee complies with all applicable laws and regulations, conditions of licensure, and directives issued by the LGA.[249]

As to the licensing procedure, an application for any of the four classes of remote gaming licence requires remittance of a €2,330 fee.[250] This covers the administration cost and costs of investigation. This is a low fee and may not sufficiently defray thorough investigation costs. There appears to be no separate fee required for key officials in respect of each licensee. However, the Malta Regulations also permit the LGA to requisition actual investigative, inspection, and other costs from the licensee or proposed licensee "when objectively reasonable."[251] Interestingly, the fee schedule also calls for special fees (sometimes based on an hourly rate)[252] when the LGA must review and pre-approve a contractual relationship between a licensee and a supplier.[253]

---

[242] Remote Gaming Regulations, S.L. 438.04 (2004) (Malta), *available at* http://www.lga.org.mt/lga/content.aspx?id=87374 (follow "Remote Gaming Regulations English Version").

[243] *Id.* §§ 7–8.

[244] *Id.* § 13.

[245] *Id.* § 4.

[246] *Id.* 1st Sched. Reg. 3.

[247] *Id.* § 15(1).

[248] *Id.* § 15(2)(a).

[249] *Id.* § 15(2)(b).

[250] *Id.* 2nd Sched. Reg. 6, § 1.

[251] *Id.* § 6(3).

[252] *Id.* 2nd Sched. Reg. 6, § 5.

[253] *Id.* § 11(4)(e). Note that this provision only applies when the supplier is to receive a percentage of the profits of the remote gaming operation or a commission.

The application form itself solicits useful information. For example, it requires a listing of "all proposed/registered beneficiaries" of the corporate applicant. Presumably this means all of the registered shareholders of the corporation, not merely those over a particular threshold percentage. The application also seeks disclosure of particulars concerning patents and trademarks proposed to be used in connection with the licensed Internet gaming operations. However, the key official personal declaration form may not elicit some useful pieces of information. The application seeks information about previous assignments in bankruptcy of the individual, for instance, but does not expressly solicit full financial statements from the prospective key official.

With suitability out of the way, the money laundering rules and procedures should be examined. The LOGA provides that, notwithstanding the provisions of the Prevention of Money Laundering Act (the "**PMLA**")[254] the Minister of Finance may provide guidelines for gaming licensees and their employees in relation to transactions that may give rise to money laundering suspicions.[255] (No such specific guidelines for gaming licensees have been issued.) The LOGA also mandates that, where any employee of the LGA and any "officer or employee of a licensee or other person acting on behalf of a licensee or under an arrangement with him" has reason to suspect a money laundering transaction has taken place or will take place, that person has an affirmative duty to act in accordance with regulations made under both the PMLA and the LOGA.[256] Note that the Malta Regulations also mention money laundering generally, *e.g.*, whether the applicant has followed policies and will take affirmative steps to prevent money laundering is one of the fit and proper tests.[257]

An interesting dynamic between the PMLA and the more specific gaming regime is worth mentioning here. While the foregoing provisions appear to imply that Internet gaming licensees are within the ambit of the PMLA, the Prevention of Money Laundering and Funding of Terrorism Regulations (the "**PMLA Regulations**") only define "relevant activity" as including the activities of "casino licensees."[258] ("Subject persons" include persons

---

[254] Prevention of Money Laundering Act (Malta), *available at* http://justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8842&l=1.

[255] Lotteries and Other Games Act (Malta), *supra* note 238, § 61(1).

[256] *Id.* § 61(2).

[257] Remote Gaming Regulations, *supra* note 242, § 8(2)(g).

[258] Prevention of Money Laundering and Funding of Terrorism Regulations, S.L. 373.01 (2008) (Malta), § 2(1)(g) (definition of "relevant activity"), *available at* http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=10454&l=1.

carrying out relevant activities.[259]) In the PMLA Regulations, "casino" has the same meaning as in Malta's Gaming Act[260]—and "casino licensee" is construed accordingly[261]—but the Gaming Act only says that "'casino' means such premises in relation to which the Minister [of Finance] has granted a concession," which does not expressly include remote gaming.[262] Accordingly, it seems open to question whether or not Internet gaming licensees are specifically subject to the provisions of the PMLA and the PMLA Regulations. Irrespective of any ambiguity, and given the application of the Third Directive to "casinos" in Malta, as Malta is a full EU member, as a practical matter it appears that local counsel and operators in Malta *act as though* the provisions of the PMLA and the PMLA Regulations apply to Internet gaming licensees in Malta.[263] Obviously, any confusion or lack of clarity on this point is less than ideal from a best practices perspective.

With respect to specific guidance similar to what has been produced by Alderney and the Isle of Man, the Financial Intelligence Analysis Unit (the "**FIAU**") in Malta, which is the country's designated FIU mandated by the FATF, has issued a series of Implementing Procedures (the "**Malta Guidance**").[264] The Malta Guidance is an attempt by the FIAU to outline the requirements and obligations of the PMLA and the PMLA Regulations and assist subject persons in designing and implementing systems and controls for the detection and prevention of money laundering and terrorist financing.[265] The Malta Guidance effectively appears to adopt a risk-based approach at one stage,[266] and requires the implementation of procedures to manage the money laundering risks posed by each subject person's customers,[267] but it also expressly states that the risk-based approach itself is optional.[268]

---

[259] *Id.* § 2(1) (definition of "subject person").

[260] Gaming Act (Malta), *available at* http://www.justiceservices.gov.mt/DownloadDocument.aspx?app=lom&itemid=8867&l=1.

[261] Prevention of Money Laundering and Funding of Terrorism Regulations, *supra* note 258, § 2(1) (definition of "casino").

[262] Gaming Act (Malta), *supra* note 260, § 2 (definition of "casino").

[263] Interview with Olga Finkel, Managing Partner, WH Partners (Mar. 20, 2012).

[264] Implementing Procedures Issued by the Financial Intelligence Analysis Unit in Terms of the Provisions of the Prevention of Money Laundering and Funding of Terrorism Regulations—Part I (2011), *available at* http://www.fiumalta.org/library/PDF/23.08.2011%20-%20Implementing%20Procedures%20-%20FINAL%20%28With%20amendment%20dates%29.pdf [hereinafter Malta Guidance].

[265] *Id.* at 10.

[266] *Id.*

[267] *Id.* at 54.

[268] *Id.* at 57.

The Malta Guidance sets out certain customer due diligence procedures that would appear similar to those adopted in the Isle of Man. Recall that the Isle of Man required the full name, residential address, date of birth, place of birth, and nationality of each player at account setup in for a B2C licensee. The more general identification requirements in the Malta Guidance require official full name; place and date of birth; permanent residential address; identity reference number, where available; and nationality.[269] The only additional requirement is the identity reference, but no documents need be tendered to an online gaming licensee at this stage. Verification of identity (for example, when there is a deposit or withdrawal of €2,000 or more, consistent with both the Third Directive and the provisions of subsection 9(1) of the PMLA Regulations) procedures include submission of valid government-issued identification documents to the gaming licensee.[270] Extra due diligence is recommended to be undertaken in the case of PEPs,[271] and extra caution is suggested in relation to business relationships with persons from jurisdictions that are not "reputable jurisdictions."[272] The Malta Guidance also asserts that subject persons should pay special attention to any money laundering threat that may arise from new or developing technologies or from products that may favour anonymity.[273]

The Malta Guidance also contains sundry record-keeping requirements. These include items like customer due diligence documents obtained by the licensee and details on transactions—presumably including withdrawals and deposits—by players.[274] Consistent with the regime set out by the FATF on records retention, the Malta Guidance establishes that these records are to be retained for no less than five years.[275] Note that the Malta Regulations also set out data retention requirements with respect to financial reports[276] and about each game played in the gaming system itself (including, *inter alia*, player balances, stakes played, and results).[277]

---

[269] *Id.* at 20.

[270] *Id.* at 20–22.

[271] *Id.* at 50.

[272] *Id.* at 38. "Reputable jurisdiction" in § 2 of the PMLA Regulations means "any country having appropriate legislative measures for the prevention of money laundering and the funding of terrorism, taking into account that country's membership of, or any declaration or accreditation by, any international organisation recognised as laying down internationally accepted standards for the prevention of money laundering and for combating the funding of terrorism, and which supervises natural and legal persons subject to such legislative measures for compliance therewith."

[273] Malta Guidance, *supra* note 264, at 50.

[274] *Id.* at 65–66.

[275] *Id.* at 67.

[276] Remote Gaming Regulations, *supra* note 242, 3rd Sched., Reg. 25, § 7.

[277] *Id.* § 9.

A money laundering reporting officer is to be appointed for each licensee.[278] Consistent with other reporting officer relationships that we have seen, this officer must occupy a senior position within the organization where she can effectively influence the subject person's anti-money laundering policy.[279] The money laundering reporting officer must have a direct reporting line to the enterprise's directors and possess the authority to act independently in carrying out her responsibilities.[280] Furthermore, licensees are required to ensure that employees are aware of the organization's anti-money laundering policies and to train their employees in recognizing and handling suspicious transactions.[281] External reporting of suspicious transactions to the FIAU are addressed in subsection 15(6) of the Malta Regulations and in greater detail in the Malta Guidance.[282] Tipping off offences are briefly covered in the Malta Regulations.[283]

With respect to financial intermediaries working with Internet gaming operators, they are not specifically addressed in the Malta Guidance. (No part of the Malta Guidance appears specifically directed at online interactive gaming licensees, perhaps owing to the ambiguity in whether the PMLA applies to the LGA's remote gaming licensees in the first place.) The Malta Guidance establishes certain customer due diligence measures undertaken by intermediaries that can be relied upon by licensees in certain circumstances, but does not allow subject persons to rely on ongoing monitoring measures carried out by another subject person or third party.[284]

Finally, Malta maintains a series of current international lists identifying various parties subject to sanctions or other restrictive measures.[285]

---

[278] Malta Guidance, *supra* note 264, at 70.

[279] *Id.*

[280] *Id.*

[281] *Id.* at 82.

[282] *Id.* at 72–75.

[283] Remote Gaming Regulations, *supra* note 242, § 16(1).

[284] Malta Guidance, *supra* note 264, at 51. There is a limited exception to the customer due diligence requirements where the third party undertakes currency exchange or money transmission or remittance services, but the exception only applies if the subject person relying on the third party is itself a financial institution whose main business is currency exchange or money transmission or remittance services. Malta Guidance, *supra* note 264, at 52. Clearly such an exception does not apply to Internet gaming operators licensed by the LGA.

[285] Malta Financial Services Authority, International Sanctions, *available at* http://www.mfsa.com.mt/pages/viewcontent.aspx?id=105.

4.6. Nevada

The final jurisdiction in our survey is the U.S. state of Nevada. In many ways, Nevada exemplifies best practices. Nevada—and specifically Las Vegas—is almost a metonym for international bricks and mortar gambling, or at least for land-based gambling in the United States. Thus far, Nevada has elected to actively regulate and accept applications for licensure in respect of intra-state interactive poker only.[286] Nevada's interactive gaming regulations allow for three basic types of licence: an interactive gaming operator licence;[287] a licence to manufacture interactive gaming systems;[288] and, a service provider licence.[289]

The process for determining suitability in Nevada is impressive and expensive. The initial licence fee for an establishment to operate interactive gaming is US$500,000.[290] The inquiries and investigations made by the state Gaming Control Board (the "**GCB**") are extensive and the burden of proof with respect to granting any licence is at all times on the applicant.[291] As far as investigations, these costs (accumulated on an hourly basis by GCB agents) are fully charged to an applicant for licensure. Estimates of investigatory costs "can be very high and range from $30,000 for a very simple investigation to over a million dollars for a complex investigation involving foreign citizens. In addition, the costs of investigating the corporation often exceed $50,000 to $100,000."[292] Investigations do not begin unless and until the estimated investigation fees are paid.[293] Historically, every shareholder of a private corporation applying for a nonrestricted licence in Nevada had to be found suitable by the GCB. However, recent amendments to the Nevada Gaming Control Act and attendant regulations now allow persons holding five per cent or less of the issued and outstanding shares of a private licensee to merely register with the GCB and submit to its jurisdiction.[294] That said, whether a corporation seeking a nonrestricted licence is publicly

---

[286] Nev. Gaming Comm'n. Reg. 5A.140(1)(a) (2011) (providing that operators shall not accept or facilitate wagers "on any game other than the game of poker and its derivatives as approved by the chairman and published on the board's website").

[287] Nev. Gaming Comm'n. Reg. 5A.030 (2011).

[288] Nev. Gaming Comm'n. Reg. 14.020 (2011).

[289] Nev. Gaming Comm'n. Reg. 5.240(2)(d) and Reg. 5.240(3).

[290] Nev. Rev. Stat. § 463.765 (2001); Nev. Gaming Comm'n. Reg. 5A.040 (2011).

[291] *See, e.g.* Nev. Gaming Comm'n. Reg. 15.1594–4 (1973).

[292] Anthony Cabot, Obtaining a Non-Restricted Gaming License in Nevada 6 (n.d.).

[293] *Id.*

[294] *See, e.g.* Nev. Rev. Stat. § 463.5735 (2011). Nevada Senate Bill 218 was signed into law on May 16, 2011.

traded or not, the GCB has the authority to require any person holding any beneficial interest in the licensee to undergo a full finding of suitability.[295]

The investigation itself is clearly thorough. Disclosure through the Multi-Jurisdictional Personal History Disclosure Form, for example, touches on everything that is relevant from a suitability perspective, as befits its length (the form itself, plus relevant attachments, can easily run into the hundreds of pages). A suitability investigation will go into every aspect of an applicant's finances.[296] Anecdotes about the bizarre things arising in investigations are legion, *e.g.*, the team of agents flying to the east cost of the U.S., auditing a safe deposit box of an applicant at a bank, and discovering US$25,000 labelled "payoff funds."[297]

An application for licensure as an operator of interactive gaming in Nevada will be made, processed, and determined in the same manner as a nonrestricted gaming licence application.[298] The same high (nonrestricted gaming licence) standard applies to a licence to be a manufacturer or distributor of an interactive gaming system[299] and to any service provider who receives payments based on earnings or profits from any gambling game (including, for example, marketing affiliates paid a percentage of rake on an interactive poker network).[300]

Anti-money laundering mandates and rules in Nevada come from two primary sources: the federal Bank Secrecy Act of 1970 (the "**BSA**")[301]—as amended by subsequent enactments, including the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001—and the provisions of the state gaming regulations and Minimum Internal Control Standards (the "**MICS**") (collectively, the "**Nevada Regulations**").[302]

With respect to the BSA, "a casino, gambling casino, or gaming establishment" is included in its provisions if it has annual gaming revenue in excess of US$1 million and: is licensed as a casino, gambling casino, or gaming establishment under the laws of any U.S. state or political subdivision thereof; or, is an Indian gaming operation conducted under or pursuant to

---

[295] *See, e.g.* Nev. Rev. Stat. §§ 463.5735(3) (2011) and 463.643(1)–(2) (2011).

[296] Cabot & Kelly, *supra* note 3, at 137.

[297] *Id.*

[298] Nev. Gaming Comm'n. Reg. 5A.030(2) (2011).

[299] Nev. Gaming Comm'n. Reg. 14.020(2) (2011).

[300] Nev. Gaming Comm'n. Reg. 5.240(3)(a)(ii) (2011) and Reg. 5.240(7)(a) (2011).

[301] For a useful overview of the BSA provisions, *see generally* Michael Gordon et al, *Panel Discussion: Money Laundering, Cybercrime and Currency Transactions*, 11 U.S.-Mex. L.J. 219, 219–220 (2003).

[302] Nev. Gaming Comm'n. Minimum Internal Control Standards (2012).

the Indian Gaming Regulatory Act (other than an operation that is limited to class I gaming).[303] Casinos and card rooms subject to the BSA must:

1. collect information and make reports about currency transactions—including cash in and out, the purchase of chips, safekeeping deposits, and marker purchases—in excess of US$10,000, whether the transaction is suspicious or not;[304]
2. report any suspicious transactions, with provisions that no person involved in the transaction is to be notified that the transaction has been so reported (tipping-off);[305]
3. set up "anti-money laundering programs including, at a minimum, the development of internal policies, procedures, and controls; the designation of a compliance officer; an ongoing employee training program; and an independent audit function to test programs;"[306] and,
4. consult lists of known or suspected terrorists (*e.g.*, the OFAC's Specially Designated Nationals List) to determine if anyone seeking to open an account appears on such a list.[307]

We will return to some specific BSA requirements and how they are integrated with the overall Nevada approach to suppressing money laundering in online gaming.

The Nevada Regulations establish that operators are to implement procedures that are designed to detect and prevent transactions that may be associated with money laundering and other criminal activities and to ensure compliance with all federal money laundering laws.[308] In other words, Nevada law compels compliance with its own money laundering regime and the BSA, among other statutes. This broad mandate is given specific effect throughout the Nevada Regulations.

One example of this specificity is the customer due diligence to be performed on player registration. At the creation of a player's authorized interactive gaming account, the Nevada Regulations set out information that must be collected by an interactive gaming operator. This information includes the player's name,[309] physical address where the player resides,[310] date of birth,[311] and the player's social security number (if a U.S. resident).[312] It

[303] 31 U.S.C. § 5312(a)(2)(X) (2006).
[304] 31 U.S.C. § 5313(a) (2006); 31 C.F.R. § 1021.311 (2011).
[305] 31 U.S.C. § 5318(g).
[306] 31 U.S.C. § 5318(h)(1).
[307] 31 U.S.C § 5318(l)(2)(C).
[308] Nev. Gaming Comm'n. Reg. 5A.080 (2011).
[309] Nev. Gaming Comm'n. Reg. 5A.110(2)(a) (2011).
[310] Nev. Gaming Comm'n. Reg. 5A.110(2)(c) (2011).
[311] Nev. Gaming Comm'n. Reg. 5A.110(2)(b) (2011).
[312] Nev. Gaming Comm'n. Reg. 5A.110(2)(d) (2011).

also includes confirmation that the player has not been previously self-excluded[313] and is not on the Nevada blacklist.[314] However, unlike the other jurisdictions examined here, Nevada requires, within thirty days of providing registration information, that the interactive gaming operator must perform procedures to verify that information and that the operator is to limit the player's gaming account activity during that verification period.[315] Note, however, that the player may not deposit more than US$5,000 into her account during the verification period, which is a high threshold.[316] All the same, no funds are permitted to be withdrawn during the verification period, which is a good check to have in place.[317] The verification procedures are to be recorded and maintained, and the MICS suggest that, variously, credentials are to be obtained from the player and recorded and that external sources are to be used to verify the date of birth and physical address.[318] If the verification has not occurred within thirty days, the operator must, *inter alia*, immediately suspend the interactive gaming account.[319]

There are some parallel identification requirements set out in the BSA and its regulations, for example, when a report on a transaction amount in excess of US$10,000 needs to be filed. The items to be verified and recorded include name, account number, and social security number or taxpayer identification number (if any).[320] For non-residents or aliens, verification of identity "must be made by passport, alien identification card, or other official document evidencing nationality or residence."[321]

There are robust provisions for transfers of amounts as between an interactive gaming account and the same player's land-based casino account.[322] Furthermore, where a player makes an in-person withdrawal request at a bricks and mortar gaming establishment (after transferring from her interactive gaming account), certain particulars must be recorded and the player must sign for the withdrawal.[323] Identification for the withdrawing player will need to be presented at the casino.

Authorized gaming players may hold only one interactive gaming account with an operator[324] and anonymous interactive gaming accounts or

---

[313] Nev. Gaming Comm'n. Reg. 5A.110(2)(e) (2011).
[314] Nev. Gaming Comm'n. Reg. 5A.110(2)(f) (2011).
[315] Nev. Gaming Comm'n. Reg. 5A.110(5) (2011).
[316] Nev. Gaming Comm'n. Reg. 5A.110(5)(a) (2011).
[317] Nev. Gaming Comm'n. Reg. 5A.110(5)(b) (2011).
[318] Nev. Gaming Comm'n. Minimum Internal Control Standards § 76 (2012).
[319] Nev. Gaming Comm'n. Reg. 5A.110(6)(a) (2011).
[320] 31 C.F.R. § 1010.312 (2011).
[321] *Id.*
[322] *See* Nev. Gaming Comm'n. Minimum Internal Control Standards §§ 71–73 (2012).
[323] Nev. Gaming Comm'n. Minimum Internal Control Standards § 89 (2012).
[324] Nev. Gaming Comm'n. Reg. 5A.120(2)(a) (2011).

accounts in fictitious names are not allowed.[325] Funds transferred into an interactive gaming account from one financial institution may not be transferred out of the interactive gaming account to a different financial institution.[326] Transfers from one authorized player to another authorized player are not permitted (outside of wins and losses at the virtual poker tables).[327]

In addition to the suspicious activity reports required under federal law, the Nevada Regulations contain their own provisions for reporting "suspicious wagering" where the wager is suspected of being in violation of federal or state law[328] or where the wager "[h]as no business or apparent lawful purpose or is not the sort of wager which the particular authorized player would normally be expected to place, and the licensee knows of no reasonable explanation for the wager after examining the available facts, including the background of the wager."[329]

With respect to records retention, Regulation 5A.190 sets out that operators must maintain "complete and accurate records of all matters related to their interactive gaming activity," including with respect to player identities, player registration, and complete game histories for every game played on the interactive gaming system.[330] Operators must preserve these records for a minimum of five years after they are made, in line with the FATF standard.[331] The GCB also takes the view that the provisions of Regulation 6.060 (producing to the GCB audit division or the tax and license division, on request, all records required to be maintained by Regulation 6) also applies to all interactive gaming records. Regulation 6.060 also requires a five-year minimum retention period.

Finally, with regard to payment processing intermediaries deployed by an interactive gaming operator, depending upon the nature of the relationship with the operator and the intermediary's relationship to the flow of funds between operator and customer, Nevada regulators may require licensure of the processor either as a Class 1 service provider (*i.e.*, required to submit to the same process as a nonrestricted licence applicant) or as a Class 2 service provider (*i.e.*, only required to make a restricted licence application). At the time of writing, the situation is unsettled. Irrespective of how such intermediaries will be licensed, however, Nevada will take a strong interest in vetting and monitoring the payment processors used by operators. For example, section 82 of the MICS requires that the interactive gam-

---

[325] Nev. Gaming Comm'n. Reg. 5A.120(3) (2011).
[326] Nev. Gaming Comm'n. Reg. 5A.120(7) (2011).
[327] Nev. Gaming Comm'n. Reg. 5A.120(9) (2011).
[328] Nev. Gaming Comm'n. Reg. 5A.160(1)(a) (2011).
[329] Nev. Gaming Comm'n. Reg. 5A.160(1)(b) (2011).
[330] Nev. Gaming Comm'n. Reg. 5A.190 (2011).
[331] *Id.*

ing operator's internal control standards delineate: procedures established for the use of each payment processor;[332] and, all deposit methods available to authorized players and a complete description of the entire process for each method.[333]

Nevada has clearly consulted widely and factored key best practices into the Nevada Regulations, particularly on suitability and customer due diligence. When the Nevada rules are considered alongside the BSA, it forms an impressive bulwark against money laundering. We will see the influence of Nevada in the best practices adopted as recommendations in the next section.

5. Thoughts on Best Practices

This paper has canvassed some definitions and methods of money laundering and pinpointed why money laundering should be challenged. With full knowledge of the limitations of what Internet gaming regulators can actually do to control the problem, we have very briefly assessed the approach of several jurisdictions to transaction handling and preventing money laundering. Many of the various regimes reflect principles and procedures set out in the 40 Recommendations.

We now turn to the key best practices put forward and advocated by this paper. Nevada is clearly the gold standard because of its high standards and 'closed' nature (*i.e.*, none of the underlying gaming transactions themselves are illegal in Nevada, so there should be no risk of the gaming activity itself generating illicit funds). The Nevada example is heavily leveraged in our best practices. Not surprisingly, given the breadth of the FATF's recommendations—and the depth and expertise of the FATF itself—many of these calls for best practices will also reflect the 40 Recommendations. The suggested best practices for currency and transaction handling and preventing money laundering in online gaming will be grouped into five main areas: regulating the sector; adopting a dynamic, risk-based approach; transparency of all participants; traceability of all transactions; and, control of operators by regulators and security of their operations. Almost any taxonomy will generate overlap. For example, regulation strongly implies assessments of suitability, but suitability assessments will be covered under the rubric of transparency. Also, should knowing the sources of client funds be grouped with transparency or traceability? (In this list, they are put under traceability because that category tracks transactions through the financial system, from their original sources through subsequent Internet gaming operations. However, the clear role of knowing the client and how the client obtains her

[332] Nev. Gaming Comm'n. Minimum Internal Control Standards § 82(a) (2012).
[333] Nev. Gaming Comm'n. Minimum Internal Control Standards § 82(b) (2012).

funds is acknowledged.) Some comments are made on each of the categories.

5.1. Internet Gaming Should be Regulated

This seems tautological; best practices for regulation assumes regulation. However, it is not universally agreed that the industry should be regulated at all. Many continue to believe that Internet gaming should be banned outright or that it should be ignored by policy makers. For example, there are several states in the US and provinces in Canada with land-based casinos that do not have a fully-functioning and local government-sanctioned online gaming model in place. Some large countries (*e.g.*, India and China) do not have a regulated Internet gaming and betting industry at all. From an anti-money laundering standpoint only, the need for regulation of the industry seems clear. Simple prohibition seems to increase the chances for money laundering; regulation cuts against this. However, regulators must be appropriately funded in order to properly undertake their work. Regulation of the industry requires continuing resources and commitment by policy makers.

Recommendation 28 in the 40 Recommendations clearly establishes that Internet casinos "should be subject to a comprehensive regulatory and supervisory regime" ensuring they have effectively implemented the necessary components of the FATF recommendations.[334] Minimum requirements are that Internet casinos be licensed by competent authorities.[335] The rationale for this kind of approach ranges from the preservation of freedom to undertake activities that many find unobjectionable—while minimizing or "managing down" collateral harms[336]—to the intuitive futility of trying to completely prohibit those activities.[337]

Strictly from the perspective of preventing money laundering, the case for regulation of the Internet gaming sector is strong. According to Cabot and Kelly, there is agreement among experts that if land-based "casinos are to be kept free of criminal domination and its association with money laundering, they must be subject to strong administrative control."[338] There is no principled reason to doubt that the same normative connection to strong regulation has any less applicability to preventing money laundering in

---

[334] Financial Action Task Force, International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation—The FATF Recommendations, *supra* note 17, at 23.

[335] *Id.*

[336] *See, e.g.* Levi, *supra* note 9, at 26.

[337] *See, e.g.* K. Alexa Koenig, *Prohibition's Pending Demise: Internet Gambling & United States Policy*, 10 Pitt. J. Tech. L. & Pol'y 1, 36–37 (2009–2010).

[338] Cabot & Kelly, *supra* note 3, at 136.

online context and, in fact, the authors go on to note the negative relationship between strong Internet gaming regulation and money laundering opportunities.[339] The other thing to note from Cabot and Kelly's statement is that it implies a role for regulators transcending suitability assessments; suitability is a necessary but not sufficient precondition for preventing money laundering.[340]

Regulation of the sector suggests that a blanket prohibition will not work, even if that is desirable as a matter of principle. One example of the United States' attempt at prohibition is the Unlawful Internet Gambling Enforcement Act (the "**UIGEA**").[341] The irony of the approach adopted in the UIGEA is that it makes money laundering easier and more likely by prohibiting involvement of the regulated credit card industry, for example, in transferring funds to online gambling websites.[342] (Put more broadly, prohibiting instead of regulating Internet gaming discourages legitimate U.S. casino operators from entering the market while encouraging "entry by unlicensed, unregulated, and unknown 'fly-by-night' entities."[343]) Before and after its passage, many predicted that the UIGEA would lead to the creation of complicated and unregulated processes for transferring funds to US-facing Internet gaming sites.[344] For good measure, one might have added that these alternative processes might also be illegal.[345] Poor regulatory oversight, among other things, helps money laundering thrive.[346]

Proper regulation does not mean only setting up the proper structure for online gaming and betting. It means an ongoing monitoring role consistent with Cabot and Kelly's "strong administrative control." It is also critical for regulators to have stable and sufficient funding for their activities and operations. Without proper resources, a great regulatory framework may be

---

[339] *Id.* at 144–145.

[340] *See also id.* at 139: "Admittedly, the problem of money laundering may still remain notwithstanding the suitability of gaming operators."

[341] *Supra* note 50.

[342] Katherine A. Valasek, Comment, *Winning the Jackpot: A Framework for Successful International Regulation of Online Gambling and the Value of the Self-Regulating Entities*, 3 Mich. St. L. Rev. 753, 765 (2007).

[343] Schwartz, *supra* note 51, at 128. *See also* Koenig, *supra* note 337, at 36–37.

[344] *See, e.g.* Valasek, *supra* note 342, at 765. *See also* Susan Ormand, Comment, *Pending U.S. Legislation to Prohibit Offshore Internet Gambling May Proliferate Money Laundering*, 10 Law & Bus. Rev. Am. 447, 451 and 453–454 (2004). (Ormand made substantially similar points about the UIGFPA in 2004.)

[345] One can view the Internet gaming indictment in the Southern District of New York in April 2011 in precisely this context. *See* Superseding Indictment, United States v. Scheinberg et al, 10 Cr. 336 (S.D.N.Y., 2011).

[346] Valasek, *supra* note 342, at 765.

completely ineffective.[347] In fact, as we have already seen, the IMF saw a lack of regulatory resources sufficient to meet the growth of the Internet gaming sector as worthy of comment in the case of the GSC.[348]

Accordingly, the first best practice is that the Internet gaming and betting sector be subject to robust regulation, extending from assessments of suitability through to effective, ongoing, and random inspection and audits. Note that regulation of MVTS, consistent with recommendation 14 of the 40 Recommendations, is also desirable. Regulation of such bodies will be done, at least in part, by non-gaming regulators. (See the example of PayPal, which is discussed in section 6.1, below.) Whether any particular MVTS is regulated or not—and the quality of that regulation—should be considered by Internet gaming regulators. More regulated and reputable MVTS businesses should be looked upon more favourably by regulators and operators than less regulated and reputable solutions, consistent with a risk-based approach. Regulators must also be suitably funded in order to do their work properly.

5.2. Adopt a Dynamic, Risk-Based Approach

Regulators ought to implement a risk-based approach that is dynamic and flexible enough to adapt to changing circumstances. This is imperative in an industry that is as subject to technology innovations as the Internet gaming sector. A risk-based approach does not mean a lack of minimum standards or a subjective view of what constitutes "risk." However, it does mean that, on top of minimum thresholds, which are themselves subject to constant refinement, limited resources of states, regulators, and operators should be deployed where they will have the most impact and away from areas that are of comparatively little concern.

Why adopt a risk-based approach? Would an accounting audit check-box type of standard work just as well while providing clearer guidance? The answer can be found in the roots of the industry requiring regulation and, indeed, in the nature of electronic commerce itself. Money laundering threats change constantly and vary across customers, jurisdictions, products, delivery channels, and over time.[349] For instance, money laundering risks may be very different in peer-to-peer games than in house-banked games or certain sports bets. Increased mobile phone and technology pene-

---

[347] Cabot & Kelly, *supra* note 3, at 137–138 (discussing the effects of a lack of resources in various quarters on land-based casino gaming regulation in New Jersey).

[348] *See supra* text accompanying note 215.

[349] Remote Gambling Association, Anti-Money Laundering: Good Practice Guidelines for the Online Gambling Industry ¶ 27, *available at* http://www.rga.eu.com/data/files/rga_aml_guidance_2010.pdf.

tration might offer more anonymous payment options that are already present in a mobile market and that may have been initially vetted for uses other than Internet gaming; certain types of prepaid phone cards are examples of such 'crossover' technology. In this environment, the regulatory response must be as dynamic as the criminal laundering element, and a prescriptive and static check-box standard would likely be off-target and would not deliver benefits greater than the costs of intervention and regulation.[350] As one author succinctly puts it, the online interactive gaming business is a "stunning example of technology outpacing the law."[351] The law needs to be clear and rational enough to squarely address existing threats, but also needs to be flexible in order to match the pace of technological and market change. Consistent with these comments and with the FATF's recommendation 15, regulators should approach new technologies that favour anonymity or that otherwise challenge or undercut effective anti-money laundering procedures with particular care.

The risk-based approach advocated here is the same as that adopted in the 40 Recommendations (see section 4.1, above). A risk-based approach starts with a risk analysis or assessment to determine areas of particular vulnerability or concern. The approach then seeks to ensure that that adopted measures to prevent money laundering are both rationally connected and proportional to the identified risks. In the words of the FATF, "[t]his will allow resources to be allocated in the most efficient ways. The principle is that resources should be directed in accordance with priorities so that the greatest risks receive the highest attention."[352]

However, it is critical to note two things about a risk-based approach. The first is that the concept of risk is not subjective or defined by one person or institution. While there is certainly room for debate in determining whether certain industries pose higher or lower risks, for example, the concepts of risks employed must reflect adherence to international norms and standards, including assessments by both the FATF and the IMF. For example, it is axiomatic that large and anonymous cash transactions are higher-risk than traceable transactions through a reputable and licensed bank.

The second item to note is that a risk-based approach does not mean that there are no minimum objective standards. Indeed, the 40 Recommenda-

---

[350] *Id.*

[351] Lawrence G. Walters, *The Law of Online Gambling in the United States—A Safe Bet, or Risky Business?* 7 Gam. L. Rev 445 (2003). Another way of making the same point is as follows: "The first challenge is that there are an 'infinite' number of ways to launder money. Laundering schemes range from simple to complex … The second challenge in detecting the money laundry cycle is the vast amount of resources that traffickers can devote to innovating money laundering techniques." Bachus, *supra* note 3, at 845–846.

[352] Financial Action Task Force, RBA Guidance for Casinos (2008), *supra* note 91, at 6.

tions mandate a risk-based approach up front but go on in the remaining 39 recommendations to set out a comprehensive framework for addressing minimum standards for deterring money laundering and terrorist financing. The US$/€3,000 threshold for casinos in recommendation 22 is one example. (There is no magic in that particular figure, but it is an objectively low figure in the context of e-commerce, and the international community—through the FATF membership—did not revise that threshold in the 40 Recommendations as revised and re-issued in February 2012.) Another example is the requirement that casinos be licensed pursuant to applicable law.

Consistent with the 40 Recommendations, the risk-based approach should not dissuade us from establishing further best practices, either. Collectively, at least some of these thresholds form a floor on anti-money laundering standards in Internet gaming. In section 5.3, below, the paper sets out a proposal that, as part of knowing with whom one is dealing at all times, the OFAC's Specially Designated Nationals List (or a comparable local list) be consulted, that transactions with any persons or organizations on that list be refused, and that such transaction attempts be reported. In the section on the traceability of transactions, the article recommends that regulators must be exceedingly wary of allowing cash to be accepted by any intermediary between the i-gaming operator and the customer, at least without robust due diligence being undertaken by such an intermediary, *e.g.*, a customer depositing funds into her account at a regulated bank in the United Kingdom and then linking her account as a deposit and withdrawal method on an interactive gaming site. Neither of these recommendations is inconsistent with or detracts from a risk-based approach.

The risk-based approach also, however, presents a number of challenges that should not be ignored. For one thing, it requires sound and well-trained judgment in compliance decisions, which may be perceived as more than what is required under a prescriptive check-the-box approach.[353] Accordingly, there is a need for better trained, more expert, and therefore presumably more expensive staff with a risk-based approach. Moreover, a risk-based approach can require a fundamental shift in mindset in some organizations in terms of accepting more interpretation and analysis—some might say ambiguity—in the compliance function.

However, with all of its challenges, the risk-based approach is the approach to preventing money laundering is clearly the dominant approach and it is the one adopted here as a best practice. When layered on top of certain minimum standards and procedures and where a regulator is properly structured and funded (see section 5.1, above), any concerns about it can

[353] Financial Action Task Force, RBA Guidance for Casinos (2008), *supra* note 91, at 8–9.

be effectively addressed. Increased analysis can lead to better protocols and decisions. Increased and targeted resources in an anti-money laundering context should have salutary effects. The FATF has set out a number of specific transaction risk issues that are raised by Internet casinos. These include multiple accounts, changes to financial institution accounts, and the use of prepaid cards and electronic wallets.[354] Each of these specific risks will be addressed by the best practices set out in this paper.

A dynamic risk-based approach is a best practice for Internet gaming regulation. We have seen that this does not mean a paucity of minimum standards or an empty view of risk. Coupled with robust regulation and other best practices, it is a practical and effective way of getting resources to the areas of transaction handling regulation that need them the most.

5.3. All Participants Ought to be Transparent

In certain key respects, phrases like transparency, 'know your client,' due diligence, identification and verification procedures, and the like are all shorthand for understanding who are one's customers and business partners.[355] However, measures that are implemented so that Internet gaming operators know who they are transacting with are not enough. Some parties may be customers or business partners of licensees, while others should be outright prohibited from doing business with regulated entities. Here again, there is a mix of minimum standards and a risk-based approach at play.

Transparency into regulatory, business, and customer relationships begins with suitability assessments by regulators. In this area, of the surveyed jurisdictions, Nevada does things the best. Nevada has a comprehensive regime for assessing the suitability of operators in the state. In the application process, operators of interactive gaming are treated in the same manner as applications for unrestricted gaming licences. Accordingly, the disclosure and investigation procedures associated with the application are thorough. This extends to key people in the prospective licensee or associated with the licensee. The costs and the investigation staff employed by the NGCB indicate that Nevada regulators take the process very seriously, which is entirely appropriate from an anti-money laundering standpoint alone. As we have already seen, being careful about who is regulated is a starting bulwark against money laundering. There is no magic number in terms of how much regulators should charge to assess and investigate applicants and their re-

[354] *Id.* at 27–28.

[355] In this section, "business partners" will be used as a proxy for any number of parties interacting with licensed gaming operators, including suppliers, marketing affiliates, and business customers on a networked gaming model.

spective associates, but it must be enough to fully fund meaningful and relevant inquiries.

The next stage is assessment of who are the operator's customers and business partners. In the case of the latter, some of these parties should be licensed by regulators as service providers. Here again, Nevada, for example, requires this. Beyond licensure, however, regulators must mandate that Internet gaming operators implement checks and procedures to vet these parties. In the case of business partners, these checks include a full and robust inquiry by the operator into the nature, backers, finances, and management of the prospective business partner. Of tantamount importance are the internal and external procedures followed by the business partner in dealing with its own customers or customers of the licensee on the licensee's behalf.

Of particular concern is the case of MTVS or other financial intermediaries processing payments for Internet gaming licensees. Here, a risk-based approach should be taken. Banks in well-regulated and -regarded jurisdictions should likely be perceived as low-risk; debit and credit cards issued by such institutions and used to fund customer accounts should be seen, accordingly, through a prism of reduced risk. Beyond that, operators should use caution in selecting MTVS partners, although a service like PayPal should be seen as relatively low-risk. As we shall see in the payment intermediaries portion of this article, below, PayPal is a electronic wallet that is regulated as a money services business in the United States. When one registers and funds one's PayPal account, one must link to an already-issued credit card or bank account, meaning that PayPal itself interfaces with trusted actors in the financial system.

Internet gaming operators should approach any MTVS business or intermediary taking cash on an anonymous basis with great caution. Note that this warning would not include banks and other financial institutions performing proper due diligence on depositors, as those transactions are not anonymous. Regulators should mandate such caution for their licensees. It might be possible that MVTS that accept cash could be found to be suitable intermediaries in the context of satisfactory player due diligence by the Internet gaming operator and, crucially, comparatively low thresholds on the amount that could be deposited on a card or voucher (*i.e.*, these would need to be below the US$/€3,000 withdrawal threshold in place in the 40 Recommendations).

As to customer due diligence in a B2C gaming operation, certain procedures in place in Nevada and in the Isle of Man appear suitable. Measures should also be consistent with FATF recommendation 10. Minimal information may be acceptable at the customer registration stage, and such information need not necessarily be checked against an external database.

(That said, the Nevada example of compelling a verification check in respect of *every* player registering is a standard to which all regulators should aspire.) However, the US$/€3,000 threshold should trigger enhanced customer due diligence procedures and attempts to verify the customer's identity having regard to government-issued documents and direct contact with the customer, if necessary. In addition, the risk-based procedures of a regulated actor like Paddy Power demonstrate best practices in this category. As discussed above, these sorts attempt to identify potential issues based on deposit methods, number of deposits, excessive payment methods linked to a user, and many other risk factors.

Customers must be prohibited from establishing fictitious accounts, from having accounts in trust on behalf of others, or from setting up multiple accounts on any particular gaming site. Circumvention procedures should be in place to enforce this rule, as well. In particular, a 'one account only' policy can minimize corruption of a peer-to-peer game like poker (where one player could otherwise control two hands at a table instead of one).[356] It also minimizes the possibility of intra-account transactions that are undertaken for no objective reason other than to move funds around and attempt to obfuscate their source.

Separate and apart from risk-based approaches to dealing with certain customers, there are some customers that should be refused. Operators should be compelled to have regard to the Specially Designated Nationals List maintained by OFAC[357] and to refuse a business relationship of any kind with listed persons. Measures should also be implemented to use private or other databases to prevent circumvention of this requirement by listed persons. Obviously, the OFAC list is just one example. Regulators must comply with local law, so such a prohibited list could leverage the OFAC list, local prohibited lists—clearly such lists are in place, as we have seen—both sources, or other comparable databases of heightened criminality or terrorism. Regulators may augment such a database with their own investigative or monitoring findings, as appropriate. (This could include, for example, results of a regulator's investigation of money laundering taking place at one of its operators applied to all operators, or the results of another Internet gaming regulator's investigation applied to the home jurisdiction.)

---

[356] Collusion goes well beyond having two accounts in the same name and controlled by the same person. It can take many forms and is constantly targeted by reputable Internet gaming sites. A broader discussion of collusion in peer-to-peer games is beyond the scope of this paper.

[357] U.S. Treas., Office of Foreign Assets Control Specially Designated Nationals and Blocked Persons, *available at* http://www.treasury.gov/ofac/downloads/t11sdn.pdf.

Transparency is a key best practice for regulators. Its essence is knowing with whom one is dealing; procedures in this section are proxies or tools for obtaining that knowledge. It extends from assessments of suitability by the regulator itself to risk-based assessments and minimum due diligence and investigation standards conducted by licensees on their business partners and customers. Certain transactions and relationships should be banned outright.

5.4. All Transactions Should be Traceable

The concept of traceability is the ability to follow and, where necessary, to reconstruct transactions. Traceability is a key feature in both preventing money laundering and in investigating and prosecuting money laundering offences that have already occurred. In this section, assessments of how funds have been accumulated or received (*i.e.*, the notion of the 'sources of funds') will also be considered. The sources, recording, and tracking of money, credit, and other instruments form the bulk of the recommendations in this section.

The starting point for this discussion is the idea of financial choke points. Choke points are entryways and exits through which funds must pass as they are disseminated throughout the economy.[358] These choke points are opportunities to record transactions and customer identities, "thereby creating a 'paper trail' that can eventually be used by law enforcement to trace laundered funds to the illegal activity from which they were originally derived."[359] Placing a transaction on a credit card, depositing money to a PayPal e-wallet, and withdrawing funds from a bank are all examples of instruments passing through a choke point in the system. A great deal of money laundering seeks to simply circumvent these choke points, which is why large cash transactions and anonymous cards holding electronic money can cause concern. Anti-money laundering best practices must try to, as much as possible, herd consumers, business partners, and transactions through functioning and reliable choke points in the financial system.

Accordingly, the Isle of Man rule against licence holders accepting cash from customers and business participants is a good one and should be adopted by regulators across the board. (Where there is a parallel bricks and mortar and interactive structure, as in Nevada, rules similar to the Nevada Regulations can address transfers between land-based and Internet channels.) As an e-commerce business, this should not be a surprising recommendation, nor should it be particularly difficult for operators to live with.

---

[358] Rueda, *supra* note 3, at 9.
[359] *Id.*

The next item to consider is that of the sources of funds of a business partner or of a customer. The origin of any party's funds and establishing the identity of that party (the latter already having been addressed in section 5.3, above) is a crucial check on that party's ability to launder funds through an Internet gaming business. Both bulwarks are important and related, but they should be considered as separate, discrete tests. A customer may conclusively establish her identity, but that may say nothing about that customer's sources of funds. Examining the origin of funds may be required if red flags are raised in identifying the customer, *e.g.*, if the risk profile of the customer as a whole is raised through identity verification, then the operator should be on guard about other aspects of the customer relationship, including the customer's sources of funds.

However, even with a low risk profile and definitive identification, when transactions go above larger thresholds—such thresholds to be established by reference to international risk factors—relevant inquiries should be made into a customer's sources of funds. Such inquiries may seek to obtain proof of a customer's income or wealth and should be designed and handled carefully both to follow local disclosure and privacy laws and to conform to good business practice. Similar rules should be employed when Internet gaming licensees establish business relationships with suppliers and corporate customers, among others.

In certain circumstances, ascertaining the origin of funds has to be mandatory. For instance, consistent with the FATF's recommendation 12, this must be done in respect of PEPs. It seems only fair that PEPs should not be shut out of Internet gaming customer or business relationships, if desired by all parties to a transaction or association, but particular care must be taken to ensure that the relationship does not further corruption in the PEP's home jurisdiction, for example.[360]

Another situation that should require determination of sources of funds is where the business partner or customer of the Internet gaming licence holder is from (*i.e.*, is ordinarily resident in or has substantial connections to) a jurisdiction that is present on the FATF's counter-measures or deficiencies lists.[361] Here again, nationals or other parties hailing from those

[360] Note also that a PEP's relationship with the Internet gaming operator should be subject to enhanced ongoing monitoring, as well.

[361] At the time of writing, the jurisdictions subject to an FATF call on its members and other jurisdictions to apply counter-measures are Iran and North Korea. The jurisdictions on the FATF's deficiencies list—and that have not made sufficient progress in addressing the deficiencies or have not committed to an action plan developed with the FATF to address the deficiencies—are Cuba, Bolivia, Ethiopia, Ghana, Indonesia, Kenya, Myanmar, Nigeria, Pakistan, Sao Tome and Principe, Sri Lanka, Syria, Tanzania, Thailand, and Turkey. See Financial Action Task Force, FATF Public Statement—16 February 2012, *available at*

countries should not necessarily be shut out of customer or business relationships entirely, but a higher degree of scrutiny should apply. Note that enhanced due diligence in respect of principals from these various jurisdictions is consonant with recommendation 19, but that mandating an investigation of the sources of funds from these countries may be perceived as going somewhat beyond the current scope of the 40 Recommendations.

The penultimate issue to address in this section is that of record-keeping. The record-keeping requirement is inextricably linked to the paper trail and choke points concepts; without suitable recording of transactions at the choke points and preservation of those records, the paper trail may not be fully re-created. Accordingly, from a money laundering perspective only, the following information should be retained by Internet gaming operators for at least five years (*i.e.*, the timeframe set out in the FATF's eleventh recommendation):

1. information and copies of documents obtained in any customer or business partner due diligence process;
2. information obtained through the risk assessment process and review as it pertains to any customer or business partner;
3. the results of all inquiries into and investigations of any customer or business partner;
4. full financial details, including wiring information and financial intermediary information, of every deposit and withdrawal made by each customer; and,
5. the full records of each game or bet played by each customer, including the stakes brought to the table, the cards played and results of each hand, and funds won or lost.[362]

Copies of such records should be kept when produced to regulators or to law enforcement, unless that would be in breach of applicable law. An Internet gaming operator's regulator should, of course, receive everything it asks for and to which it is entitled. Unless otherwise prohibited, regulators should also be copied when the local FIU or other law enforcement requests assistance according to law. Regulators should mandate co-operation with international financial crime and other investigators with suitable au-

---

http://www.fatf-gafi.org/document/18/0,3746,en_32250379_32236992_49694738_1_1_1_1,00.html.

[362] Note that this five-year requirement is without prejudice to any additional requirements that may be imposed by regulators, applicable law, or other areas of the business itself. For example, auditors may want certain financial records retained for a longer period. Similarly, regulators and internal technical staff may want remote gaming and betting logs to be kept longer. The minimum five years may variously apply to the period after which a particular transaction was completed or the end of a business or customer relationship.

thority, provided that such co-operation does not conflict with an operator's other regulatory obligations.

Finally, suspicious transaction reporting, as mandated in many of the jurisdictions covered—and by the FATF—should be implemented. Such reporting should be co-ordinated through the office of the money laundering reporting officer (discussed below). Suspicious transaction reports should be made to the local FIU and to the operator's regulator whenever a transaction with, known to, or known by the operator has taken place that the operator suspects might be money laundering, having regard to the licence holder's mandated risk assessment. Based on a risk-based approach, it is possible that such a report to law enforcement should be made even if there is no financial transaction with an Internet gaming licensee, for example, where a new customer's identity cannot be sufficiently verified and a large transaction is refused by the online gaming enterprise.

Sound traceability principles require an overall effort to push Internet gaming and betting transactions through legitimate and effective choke points. This implies a prohibition on cash being accepted by Internet gaming licence holders from customers and business partners. Sources of funds should also be reasonably investigated. Record-keeping and reporting standards are also necessary and should complete any good approach to tracking the flow of funds through a regulated gaming environment.

5.5. Regulators Need to Control the Gaming Environment and Foster Security

Best practices should include some form of broad control and attempts to secure various parts of the gaming structure by regulators. Again, this category has some overlap with other sections. The starting point is a local corporation or entity requirement, wherever possible. It covers access to data by regulators and security measures to ensure that any data retained is not corrupted or accessed by unauthorized parties. In order to control the flow of information and reporting and support other best practices, it also includes appointment of a suitably-empowered money laundering reporting officer and appropriate employee training. Finally, this section makes provision for guarding the confidentiality of investigations and preventing tipping-off.

We have seen that several regulators (*e.g.*, the Isle of Man and Malta) require local corporations to be established in order to apply for and obtain Internet gaming licensure. This has the benefit of providing a corporate actor in the licensing jurisdiction with which regulators are familiar. It also, in a sense, forces the applicant to 'commit' to the jurisdiction, although this committal takes several forms, including paying the application fee and

completing the required application forms and disclosures. More to the point, the local corporation requirement means that there can potentially be a greater level of control by regulators over the licence holder. Applicable corporate law may require a corporation to have its books and records or offices in the country, the payment of local taxes, and a technology or other nexus to the regulating jurisdiction. These become instrumentalities that a regulator can reach out and influence in order to bring a recalcitrant licence holder into line, if that becomes necessary. It is also administratively easier for a regulator to co-ordinate with other local authorities to discipline an Internet gaming licensee. For this reason, local corporation nexus should always be preferred in establishing best practices for regulators.

However, in some senses a local corporation is a proxy for control; the proxy should not be confused with actual control of a licence holder. If a jurisdiction does not have the means to licence local corporations, or if it has not done so, then it may still be possible to have good control by Internet gaming regulators over the licensee, at least in principle. Gaming regulators can mandate that there be a local corporate, technology, physical office, or other presence whether there is a corporation hailing from the jurisdiction or not. Clearly a local corporation requirement makes things easier for the regulator to control. Whether there is a requirement for a corporation from the licensing jurisdiction or not, there must be suitable integration between gaming regulations and other local laws—and gaming regulations must be robust enough in their own right—to ensure that there is sufficient control of Internet gaming licence holders by their regulators.

In an anti-money laundering context, in particular, regulators must be able to reasonably and quickly access any required records, as described above, in an acceptable form. As important, Internet gaming regulators must have effective control over who has access to those records. This will provide a trail for regulators to see how records have been accessed or modified and to prevent data corruption, thus supporting the data retention recommendation. It also serves as a warranty of sorts to the betting public that its licence holders are operating in a well-run jurisdiction that takes data protection and privacy seriously.

The money laundering reporting officer function promoted by certain jurisdictions is also worth including in our list of recommended practices. The officer must have experience commensurate with a director-level role. She must also be senior enough in the organization and have a direct reporting relationship to the enterprise's corporate directors. Such an officer can be the point person and liaison for addressing money laundering and other compliance efforts with gaming regulators. This could be extended to certain global co-ordination efforts with regulators, law enforcement, and others (e.g., the FATF), thus potentially addressing money laundering's interna-

tional character. While the money laundering reporting officer works for the licence holder, sufficient independence can be written into relevant rules and procedures to ensure that she can be another lever of control for the regulator on the inside of the licensee. Aside from control, a money laundering reporting officer can be a salutary staff addition. She can lead and coordinate staff anti-money laundering training and procedures, which measures should also be mandatory.

Finally, as an adjunct to data protection and preserving the integrity of any investigation by the licensee, the regulator, or law enforcement, rules prohibiting tipping-off must be implemented. (Tipping-off is essentially a disclosure to an unauthorized person about an actual or potential money laundering investigation or that a suspicious transaction report has been filed with the FIU.) Suitable penalties for breaching tipping-off rules need to be in place. These regulations should extend to anyone with knowledge of a relevant investigative process or with a duty to report suspected activity in the organization. As the group of people with a duty to report money laundering suspicions to the money laundering reporting officer or another party according to law is potentially large, those subject to tipping-off restrictions could also be a big group. This recommendation should be backed up by protections for good-faith disclosures by any employees or agents to the relevant FIU within the scope of applicable law and professional obligations.

Sufficient control of licensees and securing of the Internet gaming regulation and operational structure is essential. Local corporation requirements are desirable but may not be essential in all cases. Regulators must have access to and control over access to data logs and records. A suitably trained and senior money laundering officer should be appointed and relevant training provided to staff. Tipping-off and confidentiality measures need to be implemented and monitored by regulators.

5.6. Best Practices Summary Table

The various recommendations in this paper can be summarized in the following table:

Table 2
Best Practices Summary for Internet Gaming Regulators

No.	Best Practice
1	*Regulation* • Establish suitable rules, procedures, and institutions to regulate Internet gaming and ancillary activity. • Regulation must be robust and continuing. • Regulators must have sufficient resources to do their jobs.
2	*Risk-Based Approach* • Assessing risk should be in accordance with international norms and standards. • Must be dynamic and flexible in order to address new risks; reject overly mechanical approaches. • Minimum standards still apply, which are also subject to constant refinement. • Pay particular attention to new technologies, especially new technologies that favour anonymity or otherwise undercut effective anti-money laundering procedures.
3	*Transparency* • Regulators must fully inquire into prospective licensees and their associates; the cost of licensure must be commensurate with a high standard. • Regulated MVTS and financial intermediaries should be favoured over unregulated parties; intermediaries accepting cash should be approached with caution. • Strong due diligence and enhanced due diligence minimums are needed. Separate from the minimum thresholds, operators must have robust internal feedback on activity that may generate risks. • Each player may have only one gaming account per operator. • Transactions and business with certain parties (*e.g.*, on the OFAC list) should be prohibited outright.
4	*Traceability* • Customers, business partners, and transactions should be funnelled through financial choke points; cash should never be accepted by Internet gaming operators from customers or business partners. • Sources of funds should be ascertained as part of a heightened risk profile and above higher transaction thresholds. Determining the origin of funds must be mandatory in certain cases. • Suitable record-keeping and suspicious transaction reporting standards are required to round out traceability of transactions.
5	*Control & Security* • Strongly prefer licensees to be locally-incorporated. In any event, ensure that regulators have sufficient levers to control and discipline its licensees meaningfully. • Regulators must have timely access to relevant records and be able to control access to those records. • A suitably trained and independent money laundering reporting officer must be appointed; other staff in the organization must receive anti-money laundering training. • Tipping-off should be prohibited and good-faith disclosures about suspected money laundering should be protected within the bounds of applicable law.

6. Selected Payment Intermediary Issues

This paper has reviewed why suppressing money laundering is important, has looked at several jurisdictions' efforts to do that through their Internet gaming regulatory structure, and has recommended a suite of best practices. We now turn to comparisons of two specific e-commerce payment intermediaries and ask how they might fare when examined through the prism of our recommendations. One of these intermediaries (PayPal) was brought to market more than ten years ago and is in use by highly regulated gaming operators. The other mechanism, Bitcoin, was only started in 2009 but has been much in the news of late. PayPal should meet the various applicable tests for being a low-risk and usable payment mechanism. Bitcoin may cause more concern.

6.1. PayPal

As discussed previously, PayPal is an electronic wallet that has been variously described as "a peer-to-peer payment system"[363] and "not electronic money *per se*" but an approximation of the use of e-money.[364] PayPal was launched in 1999.[365] PayPal initially processed Internet gaming charges but ceased to do so in 2002 upon its acquisition by eBay.[366]

PayPal is a system that allows its customers to deposit into e-wallets, *i.e.*, accounts maintained on the PayPal system that shows credits (or liabilities) to PayPal's customers, with cash held as the corresponding debits. (A PayPal customer may transfer US$100, say, from her asset account at a financial institution into another asset account, being her PayPal e-wallet account.) Once an account is established and funded, the PayPal customer can then use her funds in e-commerce and other channels to purchase goods and services. In Internet gaming enterprises where PayPal may be used, a customer may transfer funds to her online gaming account from PayPal and may withdraw to PayPal from the online gaming account. One of the attractions of using a service like PayPal is that it can be cheaper than using other forms of payment.[367]

The success of PayPal should not cause any particular concern to those seeking to suppress money laundering in the Internet gaming space. PayPal seems to be available as an e-wallet for use on Internet gaming sites in more heavily regulated markets. More important, PayPal is itself regulated in the

---

[363] Ormand, *supra* note 344, at 452.

[364] Schopper, *supra* note 3, at 318.

[365] *Id.*

[366] Ormand, *supra* note 344, at 452.

[367] On the factors favouring a move away from credit cards towards electronic wallets and other payment systems (including PayPal), *see generally* Rueda, *supra* note 3, at 29–36.

United States, for example, seeming to offer a good example of a well-regulated and supervised MVTS. PayPal has a money services business registration number issued by the U.S. Department of the Treasury and appears to be licensed in a clear majority of U.S. states.[368]

Moreover, the procedure for depositing into one's PayPal account is clearly limited. While the registration information itself is minimal, one must deposit to or withdraw from PayPal from a credit card or an account with a regulated financial institution. Sufficient due diligence is required at the credit or debit account stage, as may be. This mixture of regulation as an MVTS and interaction with licensed financial institutions, together with relevant anti-money laundering procedures on the part of Internet gaming operators, makes PayPal a comparatively low-risk payment intermediary in a well-regulated online gaming environment.

6.2. Bitcoin

By contrast, Bitcoin is an electronic money system that has received a great deal of recent attention and generated controversy. While some aspects of Bitcoin are promising and deserve praise, the difficulties associated with identifying how its users spend Bitcoins means that this technology is not suitable for use by Internet gaming operators in a controlled and monitored marketplace.

Bitcoin was invented by Satoshi Nakamoto (a "preternaturally talented computer coder," and likely an alias) in January 2009.[369] This non-fiat currency is controlled entirely by software. A total of 21 million Bitcoins are scheduled to be released through this software, almost all of them over the coming 20 years.[370] Every ten minutes, coins are distributed through a process resembling a lottery.[371] Bitcoin "miners" play this lottery over and over; the fastest computers employed by miners win the most Bitcoins being released by the software.[372]

As a store of value and a medium of exchange, Bitcoins have a mixed track record. Bitcoins started trading at less than a penny each. However, as more merchants began to accept Bitcoins, their value appreciated. By September 2011, the exchange rate for Bitcoins was US$5 (down from US$29 the previous June).[373] Interestingly, there is at least one Internet betting website, btcsportsbet.com, operating exclusively using Bitcoins.

---

[368] PayPal, PayPal State Licenses, *available at* https://www.paypal-media.com/licenses.

[369] Joshua Davis, *The Crypto-Currency: Bitcoin and its mysterious inventor*, The New Yorker, Oct. 10, 2011, at 62.

[370] *Id.*

[371] *Id.*

[372] *Id.*

[373] *Id.*

According to its inventor, Bitcoin was developed to address "the inherent weaknesses of the trust based model" of electronic commerce.[374] Central banks must be trusted not to debase a currency, and retail, commercial, and other banks must be trusted to safeguard money on behalf of customers.[375] In the estimation of Bitcoin's inventor, history is littered with evidence of breaches of such trust.[376] Accordingly, Nakamoto set out to establish an electronic payment system based on cryptographic proof and not trust, allowing any two parties to transact directly with each other without a trusted intermediary (like a bank, or PayPal).[377] With Bitcoins, transactions would be non-reversible and, through encryption of each transaction, would not permit the same Bitcoin to be spent more than once (eliminating fraud).

The aspect of Bitcoin that is critical to this discussion is its anonymity, or its lack of transparency in discerning who is transacting what and when. It has been said of Bitcoin that "[b]uyers and sellers remain anonymous, but everyone [on the network] can see that a coin has moved from A to B."[378] Nakamoto avers as follows: "The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the 'tape,' is made public, but without telling who the parties were."[379]

How easily can the parties to a Bitcoin transaction be identified by law enforcement? One paper examining Bitcoin calls the anonymity in the payment system "complicated"[380] and concludes that it is possible to map many Bitcoin users to public keys and that "large centralized services such as the exchanges and wallet services are capable of identifying considerable portions of user activity."[381] An apparent member of the Bitcoin development team has been quoted as follows: "Attempted major illicit transactions

---

[374] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System 1, available at http://bitcoin.org/bitcoin.pdf [hereinafter Bitcoin Design Paper].

[375] Satoshi Nakamoto, Bitcoin open source implementation of P2P currency, *available at* http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

[376] *Id.*

[377] Nakamoto, Bitcoin Design Paper, *supra* note 374, at 1.

[378] Davis, *supra* note 369, at 65.

[379] Nakamoto, Bitcoin Design Paper, *supra* note 374, at 6. The analogy is very carefully worded, but it only works if law enforcement, the stock exchange, or other authorized parties can easily ascertain who the underlying parties are to the transaction. This is by no means clear from the use of Bitcoin.

[380] Fergal Reid & Martin Harrigan, An Analysis of Anonymity in the Bitcoin System 1, *available at* http://arxiv.org/pdf/1107.4524.pdf.

[381] *Id.* at 12.

with bitcoin, given existing statistical analysis techniques deployed in the field by law enforcement, is pretty damned dumb."[382]

Assuming without deciding that the concerns about the lack of anonymity in Bitcoin are true, the critical issue is whether deployment of statistical analysis techniques or other machinations in order to obtain this information for regulators or law enforcement should be necessary in a well-regulated Internet gaming environment. It would appear from the comments by the developers themselves and other analysts that the data is not easily producible to regulators within a short period of time. One Internet freedom advocate from Electronic Frontier Finland has expressed concerns about Bitcoin and said that "[w]e need to have a back door so that law enforcement can intercede,"[383] which is not comforting to the extent that it implies that law enforcement cannot presently intervene.

Whether data on the identity of transacting parties is difficult to obtain or unobtainable, Bitcoin poses problems. These sorts of barriers should not be allowed to impede the work of regulators, law enforcement, and other lawful parties. Accordingly, Bitcoin is not a technology that is ready for adoption in an online interactive gaming jurisdiction striving for best practices. In fact, Bitcoin is a great example of approaching new technologies with caution, as suggested in the 40 Recommendations and the practices adopted by this paper. Attempts to reduce fraud by not allowing the same virtual money to be spent twice are laudable, and the lack of trust in banks is understandable. Making transactions effectively non-reversible is an interesting idea, although there are consumer protection issues separate and apart from the matters raised in this paper that should be addressed. But the challenges to parties' transparency need to be met squarely before Bitcoin or equivalent substitutes can be adopted in well-regulated Internet gaming and betting.

7. The Hopes for This Paper

In this article, we have used money laundering as a way of looking at the issues around good regulation of financial transaction handling in Internet gaming. This is because of the relative importance of money laundering as an issue and the breadth of the issues raised by money laundering; it is generally instructive for currency and transaction processing requirements.

This paper has examined money laundering generally and why it matters to us. The constraints and limitations on the analysis here have been

---

[382] Adrian Chen, *The Underground Website Where You Can Buy Any Drug Imaginable*, Gawker, *available at* http://gawker.com/5805928/the-underground-website-where-you-can-buy-any-drug-imaginable.

[383] Davis, *supra* note 369, at 70.

acknowledged and explored. The FATF's 40 Recommendations and the anti-money laundering rules and procedures in Alderney, the Isle of Man, Kahnawá:ke, Malta, and Nevada have been examined. Based on the comparatives available, we have set forth some thoughts on five key best practices that regulators may be wise to adopt. Finally, two payment systems have been looked at and some thoughts given about how they stack up against good practices in terms of preventing money laundering.

Any paper like this is always part of a broader puzzle. It is not a definitive or last comment on the subject. In an industry as young, dynamic, and subject to technological change as Internet gaming, a goal like that in a mere book chapter would be overly ambitious. It is, however, hoped that this article may serve as a useful overview of anti-money laundering and financial transaction principles and good standards, as well as a spur to further and more detailed discussion among regulators, operators, and law enforcement.