Regulating Internet Gaming
 Challenges and Opportunities

Anthony Cabot and Ngai Pindell, editors

UNLV Gaming Press
A Framework for Investigating Financial Transactions and 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 do not give the issue much thought beyond the risk of fraud or counterfeiting. The sale takes place if the cash tendered is real, if the check is supported by the requisite funds, or if the credit card issuer allows the transaction. Seller and buyer are ad idem and each party gets what she wants.

Internet gaming and betting demand different considerations. 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 rarely meet their customers or even speak with them by telephone. This has implications for consumer protection measures and fraud prevention. The underlying activity (gaming and betting) is problematic. Internet gaming has only been regulated for a few years. Much of the structure people take for granted in international bricks and mortar casinos, card rooms, and sports books is still emerging in online gaming and in countries with regulated Internet gaming. Perhaps because of this, many people take the view that the online sector facilitates the transfer of illicit proceeds. Accordingly, this chapter discusses best practices in regulating transactions between licensed Internet gaming operators and their customers. This can be done through anti-money laundering initiatives.

Money laundering provides a good framework to look at financial transactions for two reasons. First, money laundering is the single biggest regulatory matter Internet gaming regulators face from a transactional standpoint. Second, money laundering is emblematic of a larger transac-
tional discussion. It draws in many issues including the best practices that affect currency and transaction requirements. It can serve as a means to focus the discussion and still generate feedback that goes beyond money laundering itself. For example, many recommendations presented here to prevent money laundering can also prevent consumer fraud. The standards adopted in this chapter provide good practices to handle general financial transactions in online gaming. For instance, reliable protocols when processing transactions require proper identification from the transacting parties and a paper trail for subsequent audit and investigation, if necessary. Therefore, the best practices to prevent money laundering also provide a viable standard into best practices for handling currency transactions.

This chapter is one small part of a larger picture and discussion. The goal here is to use proper standards to outline anti-money laundering and financial transaction principles, and to kindle further discussion among regulators, operators, professional advisors, and law enforcement. This chapter is organized as follows:

Section 2 defines the problem. It adopts a working definition of money laundering and sets out its exclusions and limitations. It also examines the various stages of money laundering and, critically, why the world places such importance on it.

Section 3 covers the constraints of this analysis and includes a discussion about the lack of understanding of the challenge of the money laundering problem in online gaming. It covers institutional and international barriers to any one regulator’s effectiveness at combating it.

Section 4 gives a very brief overview of the current rules to prevent 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, Kahnawake, Malta, and Nevada.

Section 5 discusses five key groups of best practices recommended for online interactive gaming to combat this problem:

1. Regulate the sector;
2. Adopt a risk-based approach;
3. Ensure the parties are transparent;
4. Make transactions fully traceable; and,
5. Foster control and security of the gaming environment.

Section 6 sets out two interesting payment systems in current use, PayPal and Bitcoin, then discusses each of them against the recommended standards.

Money Laundering and Why It Matters

What is Money Laundering?

The FATF states that money laundering is the processing of proceeds associated with criminal acts to disguise their illegal origin.¹ Several competing, but

broadly similar, definitions of money laundering are available. Unsurprisingly, a law and economics approach to money laundering characterizes it as a service that satisfies a direct need governed by the laws of supply and demand.

It is an offense under the Canadian Criminal Code (the “Canadian 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 offense” under the Canadian Code. A designated offense is:
  1. An offense that may be prosecuted as an indictable offense under federal law;
  2. Conspiracy to commit or attempting to commit such an indictable offense; or,
  3. Being an accessory after the fact to such an indictable offense.

In the United States, one central definition of money laundering is found in title 18, section 1956 of the U.S. Code, which “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 nature of the proceeds.” The U.S. Supreme Court has addressed the issue of whether “proceeds” within the meaning of section 1956 refers to revenues (“receipts”) or profits. Instead of agreeing on a single definition of “proceeds” for all specified unlawful activities, the Court ratified both approaches, depending on the nature of the underlying offense.

---


While many concepts of money laundering are available from statutes, international recommendations, case law, and 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 Financing7 (the “Third Directive”) is both comprehensive enough to be meaningful and concise enough to be workable. 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:

1. 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;
2. 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;
3. 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;
4. 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.

Two Limitations of the Money Laundering Definition

The definition of money laundering in the Third Directive is the definition that concerns this chapter. However, this definition presents two interesting issues:

1. What to do about money laundering where the underlying gaming transaction is illegal under domestic law?
2. Should this discussion include financing of terrorism?

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 in any particular place by accepting the bet or wager, then Art. 1(2)(c) of the Third Directive may be engaged. The operator would acquire and use customer property (i.e., funds) presumably with the knowledge 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).”

An Internet gaming regulator can and, as a matter of principle, perhaps should ensure that its interactive gaming licensees accept business only in jurisdictions where online bets are not a criminal act. The State of Nevada, for example, regulates intrastate online poker only; a Nevada gaming operator complying with local law should not deal with funds gained from an illegal bet or wager. No predicate gambling law violation exists because the interactive gaming that Nevada regulates is legal, provided it is undertaken by state-licensed operators.

A regulator may have difficulties assessing whether a foreign bet or wager is legal. Aside from principle, regulators must acknowledge the risk of over-regulation, as well. In the words of one regulator, “there is an impact to everything that we do.” If Internet gaming regulatory standards are too low, then regulators run the risk of censure by the International Monetary Fund (the “IMF”) and the FATF, among others. If regulatory standards are too high compared to other credible jurisdictions, a licensing body’s stakeholders may become dissatisfied; operators and consumers might migrate to more lightly-regulated jurisdictions. This ‘voting with their feet’ effect can lower the overall international regulatory standards, thereby hurting the consumers the regulator seeks to protect in the first place.

Is such a principled rule about definitively not allowing operators to accept business where the underlying bet or wager is or 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., the operator of www.pokerstars.com, is a licensee in the Isle of Man. Rational accepts wagers from customers in Canada, which may violate the relevant gaming provisions of the Canadian Code. Is Ratio-

---

9 Interview with Steve Brennan, Chief Executive, Isle of Man Gambling Supervision Commission (Feb. 3, 2012) [hereinafter Brennan Interview].
10 Id.
11 Id.
nal engaged in money laundering by these actions? 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 frequently. The trend among regulators will shift to increased respect for national laws and regulatory agencies, and gradually shift towards prohibiting operators from taking business in states where it may be unlawful. In the meantime, many regulators will put the burden for making these decisions on their licensees, which is easy but, on some level, unsatisfying. At the same time, operators will act unilaterally to publish and respect extensive lists of restricted territories from which they will not accept gambling transactions.

The second issue is how to combat the financing of terrorism. Until recently, the FATF had nine special recommendations designed to combat terrorist financing. In February 2012, these nine special recommendations were merged into 40 recommendations covering both money laundering and terrorist financing (the “40 Recommendations”). Concern about terrorist financing remains central to the FATF’s work.

Some safeguards used to prevent money laundering can also prevent the financing of terrorism. For example, part of “knowing one’s client” should mean checking 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 inhibits terrorist financing. However, terrorist financing and money laundering issues can be distinct. Money laundering is generally 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.” For example, “an examination of the financial connec-

---

13 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.
17 Levi, supra note 8, 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
tions among September 11 hijackers showed that most individual transac-
tions were small sums far below the reporting threshold and consisted only
of wire transfers. The individuals appeared to be foreign students receiving
money from their parents or grants for their studies.”

The FATF has not identified Internet gaming as a critical conduit for
terrorist financing. Many mechanisms are used to get money to terror-
ists, but Internet gaming is not one of them. (The hawala underground
banking system in India and Pakistan is a more noteworthy vehicle for
Al Qaeda funding.) But, as the discussion will show, money laundering
in regulated jurisdictions does not seem to be a particular problem now,
either. The best way to address terrorist financing in Internet gaming is
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. Regulators generally appear to have little appetite for
adopting such tough standards.

Some bulwarks can prevent both money laundering and terrorist fi-
nancing. Given the low reporting and enhanced customer due diligence
thresholds in some Internet gaming jurisdictions, other sectors are at
greater risk than Internet gaming. Furthermore, because both legal and
criminal activities can finance terrorism, the scope of behaviours necessary
to generate such small amounts may be “so vast that it is almost unmoni-
torable without sophisticated aggregate models and/or listing individuals
and institutions believed to constitute such a threat.” 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, some
conceptual risk remains.

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.”

18 Walters, supra note 2, at 178–179.

19 Carlson Interview, supra note 17. 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.” Testimony of
Frank Catania: Hearing on H.R. 556 and H.R. 3215 Before the H. Sub-comm. on Crime,

20 Compare Walters, supra note 2, at 171.

21 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.)

22 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.)
Money Laundering Stages

The various stages of money laundering—the process through which property is converted or transferred and its transactions concealed and disguised—are often referred to as the placement, layering, and integration stages.23

The placement stage involves the movement of proceeds—almost invariably cash24—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.25 The placement phase “is the most vulnerable to law enforcement detection because it involves the physical disposal of cash.”26 The resistance to cash as a deposit method on Internet gaming websites (except when 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 laundering. However, a barrier like this could be threatened by payment solutions that provide, for example, anonymity for their users.27

After funds have been placed into the financial system, the money launderer often 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 original proceeds from their source,28 disguise their owner, and obscure the money trail.29 This stage is seen as the most international and complex phase of the laundering cycle; funds are typically moved around multiple foreign accounts.30 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.31 Understanding the justification for currency movements and adopting standards that either prohibit or mandate operators to report suspicious transactions can prevent Internet gaming operators from being used to layer transactions.

Finally, integration is the “folded clothes” of money laundering. In this stage, “funds re-enter the legitimate economy.”32 For example, after a

23 See, e.g., Money Laundering FAQ, supra note 1; Cabot & Kelly, supra note 2, at 134; Rueda, supra note 2, at 88–91; Bachus, supra note 2, at 842–845; and, Schopper, supra note 2, at 313.
25 See Cabot & Kelly, supra note 2, at 141.
26 Bachus, supra note 2, at 842.
27 Rueda, supra note 2, at 88.
28 Money Laundering FAQ, supra note 1.
29 Bachus, supra note 2, at 844.
30 Id.
31 Id.
32 Money Laundering FAQ, supra note 1.
money launderer enters the financial system and a creates a series of movements to obscure the source of funds and ownership, either the launderer or an accomplice might withdraw funds from a bank account or investment account and use them legitimately in the economy or for purchases to further develop illegal activity and profits. Internet gaming operators’ aversion to cash transactions and the propensity to send withdrawals to licensed intermediaries provides a check point on this part of the laundry cycle. However, anonymity can cut through this barrier. Proper rules governing withdrawals, peer-to-peer transactions, and anonymity can curb integration.

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.
- Money laundering impedes economic development.

First, money laundering undermines the rule of law. Allowing money laundering to go 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 also can allow for criminal elements to acquire large sectors of an economy and corrupt public officials through the laundry. This has the potential to foster “an environment where criminal activity permeates a country’s economic and political system,” thereby undermining trust in and respect for the law.

Second, money laundering hurts business. Widespread money laundering can draw businesses into its web and make them complicit in criminality, albeit unwittingly. By undermining the financial system, money laundering also may instigate 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 abundant, they may decline investment and cut off credit. The FATF cites volatility in money demand, international capital flows, and risks to bank soundness among additional business risks. This instability and uncertainty stifle production and increases transaction costs to businesses and consumers.

Finally, money laundering hinders economic development. Shrinking businesses means aggregate output declines 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 reluctant to invest in economies fuelled by illicit funds.

33 See Bachus, supra note 2, at 845.
34 Money Laundering FAQ, supra note 1.
35 Bachus, supra note 2, at 841.
36 Money Laundering FAQ, supra note 1.
37 Id.
38 Bachus, supra note 2, at 841.
Even The Best Practices Have Constraints

The best practices to prevent money laundering have limitations. For example, the extent of the money laundering problem associated with Internet gaming is unknown. Moreover, money laundering is an international, multi-faceted, and multi-institutional issue. The best practices of one operator, or even one state, can only make a limited difference. The various constraints on what is known about money laundering and on what regulators are—or each regulator is—capable of doing must be explained before discussing current applicable safeguards and formulating a prescriptive approach to the issues.

The Size of the Problem is Unclear

Estimates of the size of the global money laundering problem vary. Several years ago, some estimated between US$300 billion and US$500 billion were laundered internationally each year.\(^\text{39}\) More recently, others relying on IMF data have suggested that the problem is 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.\(^\text{40}\) The FATF states “that overall it is absolutely impossible to produce a reliable estimate of the amount of money laundered and therefore the FATF does not publish any figures in this regard.”\(^\text{41}\) Key problems that make it hard to quantify size of global money laundering include the lack of recording basic statistics, estimation problems of yet-undiscovered criminality, and the emphasis on proving guilt over demonstrating the proceeds or profits from crime.\(^\text{42}\) 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.”\(^\text{43}\) Respective money laundering and Internet gaming experts are not aware of any figures that quantify it.\(^\text{44}\)

Many commentators presenting the risks and concerns about Internet gaming as a money laundering channel either cite conceptual concerns without any quantitative evidence or express their concerns with so many qualifications that no reasonable person would disagree. Examples are as follows:

One article cites “many prosecutors agree[ing] that it is easy and economical to launder criminal proceeds through offshore casinos.”\(^\text{45}\) However—

---

\(^{39}\) Cabot & Kelly, supra note 2, at 134; Mills, supra note 2, at 78.

\(^{40}\) Bachus, supra note 2, at 835; László, supra note 3, at 167. This range relies upon data put together by the IMF based on 1996 figures. Money Laundering FAQ, supra note 1.

\(^{41}\) Money Laundering FAQ, supra note 1.

\(^{42}\) Carlson Interview, supra note 17.

\(^{43}\) Id.

\(^{44}\) Id.; Brennan Interview, supra note 9.

\(^{45}\) Mills, supra note 2, at 78.
er, the author presents this statement without any particular discussion of exactly how the proceeds are laundered, whether it includes regulated and unregulated jurisdictions, or which offshore jurisdictions cause concern.

As a second example, the (unenacted) Unlawful Internet Gambling Funding Prohibition Act\(^46\) (the “UIGFPA”) listed the following as a congressional finding: “Internet gambling conducted through offshore jurisdictions has been identified by United States law enforcement officials as a significant money laundering vulnerability.”\(^47\) But again, the bill’s authors failed to discuss the amount of proceeds caught up in the alleged laundry.

Furthermore, Jonathan Gottfried states the following: “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.”\(^48\) For one thing, no commentator who supports legal Internet gambling would suggest that it should not be regulated; appropriate regulation of the industry is a sine qua non for preventing money laundering. For another, most serious proponents of Internet gaming oversight and control are not advocating player anonymity, especially with the transfer of “large sums of money;” unregulated or under-regulated environments that allow anonymity risk attracting criminals who engage in money laundering.

Others have arrived at more nuanced and less alarmist formulations. 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,”\(^49\) which was true in 1998 and is still true today. Two years later, the U.S. Congress’s General Accounting

---


\(^{47}\) Id. at § 2(4). See also Schopper, supra note 2, at 311, citing this provision of the UIGFPA. This finding was absent from the Unlawful Internet Gambling Enforcement Act of 2006 § 802, 31 U.S.C. §§ 5361–5367 (2006).


\(^{49}\) Cabot & Kelly, supra note 2, 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) available at http://www.oecd.org/dataoecd/13/51/34326611.pdf. 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, query how applicable those concerns are today. “Several countries” should not be taken as impugning all countries. Finally, remember that neither this chapter 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.
Office (now the Government Accountability Office) (the “GAO”) reported to Congress on some of the issues in Internet gaming. The report noted that representatives of law enforcement expressed concerns that Internet gaming could be a “powerful vehicle for laundering criminal proceeds.” At the same time, law enforcement officials conceded that no adjudicated cases involve money laundering through Internet gaming sites. By contrast, banking representatives and gaming regulators did not view Internet gaming as particularly susceptible to or as posing any particular risks in respect to money laundering. The GAO report made no recommendations to Congress. Additionally, several experts claim that money laundering is not much of a problem in regulated Internet gaming. Some offer little discussion about their assertions and conclusions; many others also offer thoughtful reasoning about why money laundering is not a material issue in regulated online gaming.

In a money laundering roundtable from three years ago, 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. Alan Pedley, an Internet gaming expert and former regulator, indicated that he had seen one instance in Australia, but 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. 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.” In an MHA Consulting report from 2009, the authors concluded that “there appears to be little evidence 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 money

51 Id. at 5.
52 “This was said to be, in part, because of a “lack of any industry regulations or oversight (emphasis added).” Id.
53 Id.
54 See, e.g. Mangion, supra note 2, 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.)
57 Id. at 280.
58 Id.
59 Id. at 282.
laundering” because the identities of gamblers are known, financial transactions are in electronic formats, and all of the wagering is recorded. Put another way, 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.”

All of these perspectives are important because regulation of Internet gaming—and implementing sound financial transaction rules—is a public policy issue. In any question about policy, one must understand the issues in order to understand the problem. 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? Do the costs of regulation versus the costs of the problem make financial sense? Does regulated Internet gaming account for half of the money laundering undertaken worldwide? Eighty per cent? Or 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 should allocate more resources to prevent it. If very little goes through a regulated Internet 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.

The absence of a working quantitative estimate is not a good reason to ignore the issue. Without a reliable measurement, however, policy makers are proceeding without useful—if not critical—information to decide how many resources they need to allocate to create rules, fund investigations and ensure ongoing compliance, that is, how to fund the legal and institutional machinery that prevents money laundering.

One Regulator’s Effectiveness is Limited

The second set of constraints on the effectiveness of regulators deals with interconnectedness; money laundering is an international and multi-institutional problem. To prevent it, operators must rely on multiple functionalities.

First, money laundering is, as recognized by the Third Directive, “frequently carried out in an international context.” As noted by the FATF, criminals will seek to exploit the differences between anti-money laundering agencies. They will move their networks and operations to states with weak or ineffective countermeasures. The movement of capital—facilitated by modern technology—makes this a continuous search by criminals for the global path of least resistance. Moreover, from an exclusively inves-

60 MHA Report, supra note 24, at 31.
61 Id.
64 Money Laundering FAQ, supra note 1.
tigative standpoint, tracking flows of cash through financial institutions is an international exercise. Effective money laundering investigations and prosecutions require the co-operation of different sovereign governments. Accordingly, an Internet gaming regulator with the best proven methods for deterring money laundering is at the mercy of the weakest link in a global financial chain. Operators 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 by the global nature of both Internet gaming and money laundering.

Second, regulatory effectiveness depends on multiple institutions; 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 that deal with Internet gaming, but the state’s banks experience a breakdown of their respective money laundering controls, then the operators could become part of an illicit laundry. For this reason, the IMF adopts a cross-institutional perspective in its various country reports.

Finally, anti-money laundering controls appeal to many facets of Internet gaming. This point can seem abstract, but consider some specific ways different factors can affect the fight against laundering. Among others, cash limits on transactions, assessments of suitability, control over local operating nexus, and the act of gaming regulation itself can affect money laundering. But what about something like location verification? This can be a serious risk factor, for example, where a customer’s location is a country on the FATF’s list of jurisdictions that require countermeasures or is on its deficiencies list. Consider an Internet gaming site’s random number generator (“RNG”). A corrupted RNG can turn a gaming website into a laundering vehicle for players or members of the operator’s staff.

The Rules

This section examines how international jurisdictions approach legal issues and handle financial transactions while preventing operators from becoming part of an illicit scheme. It starts with the FATF’s recommendations and then canvasses five jurisdictions on their approaches to money laundering controls: Alderney, The Isle of Man, Kahnawake, Malta, and Nevada.

65 Mills, supra note 2, at 84–85; Bachus, supra note 2, at 773.
67 Location verification is addressed in Chapter 11.
68 See Cabot & Kelly, supra note 2, at 144.
The FATF and the 40 Recommendations

The G7 countries established the FATF in 1989.69 The FATF was convened in response to mounting concern about global money laundering,70 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.”71 The FATF’s current mandate is to set standards and promote effective implementation of legal, regulatory, and operational measures to combat money laundering, terrorist financing, and other related threats to the integrity of the international financial system. The FATF also works with other international stakeholders to identify national-level vulnerabilities with the objective of protecting the international financial system from misuse.72

The FATF has 36 members: 34 jurisdictions and two international organizations (the Gulf Co-operation Council and the European Commission).73 The FATF works closely with eight regional bodies that are FATF associate members.74 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 instrumental in coordinating the fight against global money laundering.75 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, the 40 Recommendations represent the accepted international standards for anti-money laundering principles and procedures and have been adopted or endorsed by many nations and international bodies.76


70 About the FATF, supra note 69. See also Walters, supra note 2, at 168.

71 About the FATF, supra note 69.

72 Financial Action Task Force, Mandate (2012-2020), available at http://www.fatf-gafi.org/media/fatf/documents/FINAL%20FATF%20MANDATE%202012-2020.pdf. Today, the FATF continues to develop and promote policies to combat money laundering and terrorist financing. About the FATF, supra note 69. This it does through, inter alia, 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. Carlson Interview, supra note 17.


74 Id.

75 Rueda, supra note 2, at 16.

As one commentator noted, they “are the most comprehensive set of anti-money laundering directives yet created for governments, legislatures, law enforcement, financial institutions and businesses.”

The FATF issued a series of recommendations in 1990 to combat money laundering. These were subsequently revised in 1996 and 2003, 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. Until 2012, these collective recommendations were called the “40+9.” As previously noted, all of the FATF’s recommendations have now been consolidated into the (current) 40 Recommendations.

The FATF recommends a risk-based approach to money laundering. This is enshrined in the first of the 40 Recommendations. The risk-based approach means 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] programs adequately address such risks. Where countries identify lower risks, they may decide to allow simplified measures for some of the 40 Recommendations under certain circumstances.” The FATF calls this approach an “essential foundation” for efficiently allocating resources and implementing the 40 Recommendations. The risk-based approach is a key element of the guidance issued by the FATF for casinos.

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.”

---

77 Walters, supra note 2, at 169.
80 Id. See also 40 Recommendations (2008), supra note 16.
81 See supra text accompanying notes 15 and 16.
82 40 Recommendations, supra note 16.
83 Id. at 11.
84 Id.
85 Id.
87 40 Recommendations, supra note 6, 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
Accordingly, recommendation number 22 sets out that the customer’s due diligence and record-keeping requirements in recommendations 10, 11, 12, 15, and 17 apply to casinos, including Internet casinos. Recommendation 23 provides that the provisions for 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. In addition, recommendation 28 states that DNFBPs should be subject to regulation and supervision; this includes assessing the suitability of Internet casino owners. Finally, recommendation 14 states that providers of money or value transfer services (“MVTS”) should be licensed or regulated and compliant with relevant FATF recommendations. MVTS are businesses that accept cash and other monetary instruments, then pay corresponding sums in cash or in other forms to a beneficiary. The MVTS definition clearly includes a service like PayPal, for example.

Most FATF recommendations relevant to this chapter are summarized in Table 1.

Many of the Internet gaming jurisdictions 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.

88 Id. at 14–19.
89 Id. at 18–21.
90 Id. at 23–24.
91 Id. at 17.
92 Id. at 119.
Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.

Financial institutions 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 the 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 about 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 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 it should be required to terminate the business relationship; and, the operation should consider making a suspicious transactions report in relation to the customer.

Table 1

Selected FATF Recommendations Relevant to Internet Gaming Regulators

<table>
<thead>
<tr>
<th>No.</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>10</td>
<td>Customer Due Diligence</td>
</tr>
<tr>
<td></td>
<td>• Financial institutions should be prohibited from keeping anonymous accounts or accounts in obviously fictitious names.</td>
</tr>
<tr>
<td></td>
<td>• Financial institutions 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.</td>
</tr>
<tr>
<td></td>
<td>• The principle that financial institutions should conduct customer due diligence should be set out in law.</td>
</tr>
<tr>
<td></td>
<td>• Customer due diligence measures include the following:</td>
</tr>
<tr>
<td></td>
<td>(a) identifying the customer and verifying the customer’s identity using reliable, independent source documents, data or information;</td>
</tr>
<tr>
<td></td>
<td>(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;</td>
</tr>
<tr>
<td></td>
<td>(c) understanding and obtaining information about the purpose and intended nature of the business relationship; and,</td>
</tr>
<tr>
<td></td>
<td>(d) conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship.</td>
</tr>
<tr>
<td></td>
<td>• Financial institutions should be required to apply customer due diligence measures, but should determine the extent of such measures using a risk-based approach.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• 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 it should be required to terminate the business relationship; and, the operation should consider making a suspicious transactions report in relation to the customer.</td>
</tr>
</tbody>
</table>
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 competent domestic authorities.

12 Politically Exposed Persons

- 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 who 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 diligence 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 are 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 promptly report 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.
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 in, 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.

Alderney

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

The key piece of legislation governing Internet gaming conducted from Alderney is the Alderney eGambling Ordinance, 2009 (the “Alderney Ordinance”). Among other things, the Alderney Ordinance details two

---

93 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.


95 Id.

96 Id.

97 Id.

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). The Alderney Gambling Control Commission (the “AGCC”) is the body charged with granting and revoking licences, creating and enforcing regulations, and monitoring the industry’s licensees from Alderney. Only Alderney companies may hold Category 1 or Category 2 eGambling licences.

The Alderney Ordinance mandates that the AGCC must make regulations providing for the way in which an eGambling licensee is “obliged to take steps to comply with applicable international measures in respect of money laundering and terrorist financing.” These components are in the Alderney eGambling Regulations 2009 (the “Alderney Regulations”). The suitability requirements for licensure under licence Categories 1 and 2 are as follows:

Sections 16 and 17 of the Alderney Regulations detail the procedure for applying for a Category 1 or 2 eGambling Licence. The Alderney Regulations also set out criteria against which the applicant is to be considered. While comprehensive, the application fee to cover processing and—crucially—investigation of the applicant (£10,000) is low compared with other leading jurisdictions (e.g., Nevada). Whether a complete investigation of suitability of an enterprise can be done for this amount is an open question. The AGCC, however, may require further investigation and other costs from the applicant. The required documents for eGambling licence applicants in Schedule 1 to the Alderney Regulations are not comprehensive. For example, an applicant in Alderney only needs to disclose “known” shareholders holding 3% of the issued and outstanding share capital of the applicant or the applicant’s “parent.” Audited accounts are requested, but the application does not expressly question previous liquidation, insolvency, or bankruptcy proceedings. (Note that section 21 has “the applicant’s current financial position and financial background” as criteria against which the regulator assesses the applicant for licensure.)

100 The Alderney eGambling Ordinance, supra note 98, at §§ 4, 5, and 7.
101 Id. at § 12.
102 See, e.g. id. at §§ 4(2) and 4(3).
103 See, e.g. id. at §§ 14, 15, and 21.
104 Alderney eGambling Regulations, supra note 99, at § 3(3).
105 Id. at § 5(4).
106 The Alderney eGambling Ordinance, supra note 98, at § 22(2)(e).
108 Id. at Sched. 21.
109 Id. at § 27.
110 Id. at § 21.
When licensing key individuals, the initial investigatory and processing fee (£1,000) is low. The criteria for assessment, however, are broad and the disclosure requires more information than in the case of eGambling licence applicants. Overall, how well the Alderney rules and procedures function in terms of admitting only suitable organizations and individuals is unclear.

Other key components of the anti-money laundering protocols contained in the Alderney Regulations are in Schedule 16. Section 1 of Schedule 16 gives details on the completion of a business risk assessment as a pre-condition 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.

Category 1 (business-to-consumer) licensees must undertake customer due diligence measures:

1. Subject to section 4 of Schedule 16, before registering a customer;
2. Immediately after a registered customer makes a deposit equal to or greater than €3,000—the FATF threshold—or makes a deposit that brings the total deposits in any 24 hour period equal to or greater than €3,000;
3. When it reasonably knows or suspects that a person is engaged in money laundering or terrorist financing;
4. When it doubts the truth or sufficiency of any information previously obtained for purposes of customer identification or verification.

Operators must practice enhanced customer due diligence when a Category 1 eGambling licensee does business with a customer who is a PEP or a customer “established or situated” in a country that does not apply or insufficiently applies the 40 Recommendations.

The Alderney Regulations require each Category 1 eGambling licensee to undertake an individual risk assessment of each customer according to that licensee’s internal control systems. Alderney’s anti-money laundering guidance (the “Alderney Guidance”) states that the Category 1 eGambling licensee must collect personal information including “unique

---

111 Id. at Sched. 21.
112 Id. at § 142.
113 Id. at Sched. 9.
114 See, e.g. “high risk” customers referred to in id. at Sched. 16, § 6(1)(a).
115 Allowing identification and verification procedures after registration under certain circumstances.
116 Alderney eGambling Regulations, supra note 99, at Sched. 16, § 2(a).
117 Id. at Sched. 16, § 2(b).
118 Id. at Sched. 16, § 2(c).
119 Id. at Sched. 16, § 2(d).
120 Id. at Sched. 16, § 3(1)(a).
121 Id. at Sched. 16, § 3(1)(b).
122 Id. at § 227(2).
identifiers contained within official documents such as driver’s licences, passports or identity cards.” 123 The Alderney Guidance, however, basically leaves things up to 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.” 124 This more flexible approach was 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, and credit card information were given. 125

An example from the Alderney Guidance indicates a 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.126 In such a case, customer due diligence should be performed. By contrast, a customer depositing €2,950 and a further €100 25 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].” 127 If repeated, such transactions should be seen as higher risk under a risk-based approach.

If a Category 1 eGambling licensee cannot comply with the regular customer due diligence procedures, the licensee must not register the customer128 or must terminate the customer relationship, 129 and determine if disclosure is required130 in compliance with the Disclosure (Bailiwick of Guernsey) Law, 2007131 (the “Disclosure Law”) or the Terrorism and Crime (Bailiwick of Guernsey) Law, 2002132 (the “Terrorism Law”). General provisions in the Alderney Regulations also require that the Category 1 licensee must perform ongoing and effective monitoring of any existing custom-

124 Id. at 23.
125 This may be in accordance with, among other things, the terms of subsection 227(4) of the Alderney Regulations.
126 Alderney Gambling Control Commission, supra note 123, at 28.
127 Id.
128 Alderney eGambling Regulations, supra note 99, at Sched. 16, § 5(a).
129 Id. at Sched. 16, § 5(b).
130 Id. at Sched. 16, § 5(c).
er relationship, including scrutinizing complex or large and unusual transactions or unusual patterns of transactions (Category 2 licensees are addressed separately).

Section 7 of Schedule 16 covers reporting suspicious activities, with reference both to Part I of the Disclosure Law, which covers financial and non-financial services, and to section 12 of the Terrorism Law. Both Category 1 and Category 2 licensees must follow the reporting requirements in Schedule 16. The Alderney Regulations require both Category 1 and Category 2 eGambling licensees to appoint a money laundering reporting officer and define that officer’s responsibilities. Provisions ensure that “relevant employees” receive training in, inter alia, the Alderney Ordinance and the Alderney Regulations; internal procedures and controls to prevent money laundering; the identity and responsibility of the money laundering reporting officer; and, the detection of unusual or suspicious transactions.

For purposes of record-keeping, the rules generally require five year retention periods for both Category 1 and 2 licensees, consistent with the 40 Recommendations. For example, transaction documents or copies must be kept for five years, starting from the date the transaction and/or any related transaction(s) were completed. Licensees must retain customer due diligence information for five years starting from the date the person ceased to be a customer. The Alderney Regulations also make provisions for retaining copies of documents in case a court order requires them. The AGCC’s Technical Standards and Guidelines for Internal Control Systems and Internet Gambling Systems specify that a licensee must retain all “gambling information” (inclusive of customer account and session information) for six years. Guernsey imposes sanctions against certain blacklisted persons (notably terrorist organizations), and those sanctions apply to Alderney; therefore, Alderney must prohibit certain transactions (including gaming transactions) with or involving those persons.

133 Alderney eGambling Regulations, supra note 99, at Sched. 16, § 6(1).
134 Id. at Sched. 16, § 6(1)(c)(i).
135 Id. at Sched. 16, § 6(1)(c)(ii).
136 Id. at Sched. 16, § 6(1)(c)(iii).
137 Id. at Sched. 16, § 6(1A).
138 Id. at Sched. 16, § 7(1).
139 Id. at Sched. 16, § 8(1)(b)(i).
140 Id. at Sched. 16, § 8(1)(b)(iv).
141 Id. at Sched. 16, § 8(1)(b)(v).
142 Id. at Sched. 16, § 8(1)(b)(vi).
143 Id. at Sched. 16, § 9(1)(a).
144 Id. at Sched. 16, § 9(1)(b).
145 Id. at Sched. 16, § 9(2).
147 See, e.g. GUERNSEY FINANCIAL INVESTIGATION UNIT, Guernsey Renews Sanction Regime Al-Qaida and Taliban, available at http://guernseyfiu.gov.gg/article/6481/Guernsey-
For banking and payment processing methods and providers of 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 that 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.148

The IMF’s most recent detailed assessment report for Guernsey from January 2011 provides an objective third party view of how the AGCC is doing at deterring money laundering. While the IMF agrees that the AGCC’s supervision of interactive gaming operators is extensive,149 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.”150 Another concern raised is a request for reimbursement through a different payment mechanism than that used by a customer to deposit funds 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 of the payment mechanism is [sic] still present in absence of legislative or regulatory prohibitions.”151 The IMF also remarked on what it called “insufficient” suspicious transaction reporting by gaming operators, given the risk level and the transaction volume conducted by the industry.152

**Isle of Man**

The Isle of Man is another Crown Dependency153 in the Irish Sea between Britain and Ireland.154 As with Alderney, the UK Parliament does

---

150  Id. at 15.
151  Id. at 231.
152  Id. at 266.
153  Claire Milne, E-Gaming in the Isle of Man: A Primer, 14 Gam. L. Rev. & Econ. 371 (2010).
154  Miles Benham, The Isle of Man, in Internet Gambling Report 507 (10th ed., Mark
not legislate in respect of the Isle of Man’s internal affairs, but it is responsible for its defense and foreign affairs. The Isle of Man is not a member of the EU, but it is inside the customs union.

The Isle of Man’s Internet gaming and betting regulatory jurisdiction uses the Online Gambling Regulation Act 2001 (the “Isle of Man Act”). This outlines the Isle of Man Gambling Supervision Commission’s (the “GSC’s”) authority to issue licences to conduct online gambling, to set the conditions of licensure, and to cancel or suspend a licence. The two key classes of licence are the standard licence (for business-to-consumer operators) and the network services licence (for business-to-business operators). Both licences require a Manx corporation to be the licensee.

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—and that its activities are under the management of—persons of integrity. The application fee for a licence is £5,000, which appears low for normal investigatory costs. The government may request additional funds to defray investigatory costs if necessary. There is no fee required for investigation of key officials, which seems inadequate. The required forms for licence applicants are not onerous. For example, only shareholders with 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 there are no express inquiries about previous insolvencies or other events. Separate disclosure is required of a parent corporation, but the same five per cent rule with respect to disclosure of shareholders of the parent also is in effect. The personal declaration forms are not robust. Disclosure only of a key individual’s “main personal banking account” is required. They do not require information about other...
assets or any liabilities except for a yes/no check box concerning a default status on credit cards, mortgages, or other financial liabilities.

All licensees are under the term “licence holder” in the Proceeds of Crime (Money Laundering—Online Gambling) Code 2010 (the “Isle of Man Code”), which details procedures and rules that all licence holders in the Isle of Man must follow. The Isle of Man Code mandates that a licensee must undertake a risk assessment to determine the measures necessary when carrying out player or business participant due diligence or enhanced due diligence; the risk assessment estimates the risk of money laundering using several factors. Moreover, the Isle of Man anti-money laundering guidance (the “Isle of Man Guidance”) advocates a risk-based approach to all aspects of the Isle of Man Code. 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. It also expressly prohibits the maintenance of accounts by anonymous licensees or those who use fictitious names, in line with the 40 Recommendations.

The customer due diligence requirements in the Isle of Man are less confusing than the comparable Alderney requirements. When a player establishes an account with a B2C licensee, the licensee must “require the prospective participant to provide satisfactory information as to his identity … as soon as reasonably practical after contact is first made between them.” This means that B2C licensees 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. This is input by the player. The player does not have to 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 online gambling.” Licence holders are to establish, maintain, and operate procedures that require a customer to produce satisfactory evidence of her

---

168 Id. at § 3.
169 Id. at § 5(1).
170 Id. at § 5(2).
171 Isle of Man Gambling Supervision Commission, supra note 166, at 12.
173 Id. at § 4(1)(a).
174 Id. at § 4(1)(b).
175 Id. at § 6(1).
176 Isle of Man Gambling Supervision Commission, supra note 166, at 30; Brennan Interview, supra note 9.
identify prior to making the qualifying payment. A qualifying payment is one that exceeds €3,000, or a payment that, when taken with all other payments within thirty days preceding the date the payment is to be made, exceeds €3,000 in aggregate. This is consistent with the €3,000 threshold set for casinos by the 40 Recommendations. The documentation required here, i.e., to be “obtained and retained” by the licensee, is generally some form of government-issued identification.

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 for certain players, suppliers, and business customers is also covered; these measures apply to, among others, PEPs and to persons located in a country that the licensee has reason to believe does not apply or insufficiently applies the 40 Recommendations. Licensees also must take ongoing monitoring steps.

According to the GSC’s Chief Executive, these minimum thresholds are in line with the 40 Recommendations. He adds, however, that in applying a risk-based approach, many of Isle of Man’s licensees elect to implement further due diligence controls and identification procedures at earlier transactional stages and where increased risk is perceived. In fact, this is the case with Paddy Power, a major interactive gaming and betting operator licensed by the Isle of Man. Paddy Power, consistent with section 6 in the Isle of Man Code, obtains information at the point of registration, i.e., full name, residential address, date of birth, place of birth, and nationality. At the deposit stage, Paddy Power engages most of its risk assessment protocols. Paddy Power has a dedicated customer security team and runs constant reports based upon deposits reaching certain thresholds, and they check customers who fit various risk profiles. For example, if a new customer makes 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. (This review applies irrespective of the €3,000 threshold detailed in paragraph 7(3)(b) of the

---

178 Id. at § 7(2).
179 Id. at § 7(3)(a).
180 Id. at § 7(3)(b).
181 Isle of Man Gambling Supervision Commission, supra note 166, at 31.
182 Id.; Brennan Interview, supra note 9.
184 Id. at § 9(2)(b).
185 Id. at § 10.
186 Brennan Interview, supra note 9.
187 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.
188 Interview with Robert Reddin, Compliance Manager, Paddy Power (Feb. 10, 2012) [hereinafter Reddin Interview].
189 Id.
190 Id.
Isle of Man Code, which only applies to withdraws.) Reports are generated based on, inter alia, frequency and patterns of play, payment activities, and deposit and withdrawal methods.\textsuperscript{191} The thresholds and risk profiles in these reports are dynamic and subject to constant revision and refinement.\textsuperscript{192}

When a Paddy Power customer appears on one or more reports, the enterprise will seek to validate that customer by using a suite of tools and inquiries. This ranges from inquiries placed against external proprietary databases of information to direct questioning of the customer to determine the source of funds.\textsuperscript{193} If Paddy Power cannot ascertain the sources of funds, it will file a suspicious transaction report with the relevant Isle of Man authority.\textsuperscript{194}

According to Paddy Power’s compliance manager, who is the enterprise’s deputy money laundering reporting officer, in compliance with Isle of Man law, the vast majority of their B2C customers are electronically verified within a short period after their initial deposit to their online interactive gaming account.\textsuperscript{195}

The Isle of Man Code requires the licensee to generate and maintain records of all transactions with players and business participants sufficient to demonstrate compliance with money laundering regulations.\textsuperscript{196} These records must be kept for at least six years from: the date the player or business participant formally ceased to be a player or business participant;\textsuperscript{197} or, the date of the last transaction carried out by the player or business participant.\textsuperscript{198} The GSC takes the view that all gaming sessions on the licensee’s site are required to be tracked, recorded, and available for access by appropriate authorities to comply with the minimum six-year retention rule.\textsuperscript{199}

When reporting suspicious transactions, each licensee must appoint a money laundering reporting officer,\textsuperscript{200} who is the lynchpin of the licensee’s internal and external reporting procedures. This reporting officer must be sufficiently senior within the organization\textsuperscript{201} (or must have sufficient experience and authority, if not within the organization)\textsuperscript{202} and must have direct access to the directors or managing board of the licensee.\textsuperscript{203}

\footnotesize
\begin{itemize}
  \item \textsuperscript{191} Id.
  \item \textsuperscript{192} Id.
  \item \textsuperscript{193} Id.
  \item \textsuperscript{194} Id.
  \item \textsuperscript{195} Id.
  \item \textsuperscript{196} Proceeds of Crime (Money Laundering—Online Gambling) Code 2010, supra note 167, at § 12.
  \item \textsuperscript{197} Id. at § 13(1)(a).
  \item \textsuperscript{198} Id. at § 13(1)(b).
  \item \textsuperscript{199} Brennan Interview, supra note 9.
  \item \textsuperscript{200} Proceeds of Crime (Money Laundering—Online Gambling) Code 2010, supra note 167, at § 16(1).
  \item \textsuperscript{201} Id. at § 16(2)(a).
  \item \textsuperscript{202} Id. at § 16(2)(b).
  \item \textsuperscript{203} Id. at § 16(2)(c).
\end{itemize}
functions, the money laundering reporting officer initiates the disclosure of any applicable suspicious transaction reports to the Isle of Man Financial Crime Unit.\textsuperscript{204} Staff screening and training by a licensee 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 require a licensee to maintain appropriate procedures and controls to prevent “the misuse of technological developments for the purpose of money laundering or the financing of terrorism.”\textsuperscript{205} This is a clear call for constant vigilance about the exploitation of new technology; it demonstrates the risk-based approach adopted by the Isle of Man.

Tipping-off is covered in the Isle of Man Guidance. The offense itself is described in subsection 6.8.4(1)–(3), while the penalties associated with the offense are described in subsection 6.8.4(4). There is a current list of sanctions imposed by the Isle of Man as well as against selected territories and institutions.\textsuperscript{206}

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.\textsuperscript{207} The GSC, however, prefers a risk-based approach as advocated by the 40 Recommendations. According to the law, its licensees have a requirement in the Isle of Man to understand with whom they’re doing business. This extends to banks’ and payment intermediaries’ internal controls and procedures for their own users and customers.\textsuperscript{208} On the operator side, Paddy Power, for example, takes a risk-based approach but tries to deal with “cleaner” operators: the larger organizations that have a positive market reputation and are heavily regulated.\textsuperscript{209}

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 noted 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.\textsuperscript{210}

\textsuperscript{204} Id. at § 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 166, at 10–12.


\textsuperscript{206} Isle of Man Treasury Department, Sanctions and Export Control in the Isle of Man (2012), available at http://www.gov.im/treasury/customs/sanctions.xml.

\textsuperscript{207} Brennan Interview, supra note 9.

\textsuperscript{208} Id.

\textsuperscript{209} Reddin Interview, supra note 188.

\textsuperscript{210} IMF Isle of Man Report, supra note 66, at 20 and 207–208.
Kahnawake

The Mohawk Territory of Kahnawake is an aboriginal community of approximately 8,000 people located 20 minutes from Montreal, Canada. The entire territory occupies approximately 20 square miles. The Mohawk Council of Kahnawake (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. Kahnawake has consistently and historically asserted sovereignty over its affairs and territory. Kahnawake has its own police force, court, schools, hospital, fire services, and social services.

The Kahnawake Gaming Commission (the “KGC”) was established by the Kahnawake Gaming Law, enacted by the Mohawk Council in 1996. The KGC’s basic mandate is to regulate and control gaming within or from Kahnawake. Assessing the suitability of interactive gaming licensees and implementing money laundering controls is done under the rubric of the Regulations Concerning Interactive Gaming (the “KGC Regulations”), 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 obtained by private Internet gaming operators seeking to be “licensed” by Kahnawake. The holder of a CPA may conduct interactive gaming from Kahnawake, “but only from the co-location facility that is owned and operated by the holder of a valid Interactive Gaming Licence.”

An applicant for a CPA must complete prescribed forms and provide copious information. The data solicited in this process is extensive and useful to 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 who have provided personal information forms in addition to that application. The application cost for each proposed key person licence is US$5,000.

212 Id.
213 Id. at 322.
214 Id.
215 Id.
216 Id.
218 Id. at § 34.
219 Id. at §§ 35(a)–35(f).
220 Id. at § 35(g).
221 Id. at § 35(h).
What is much more interesting to an assessment of anti-money laundering controls in Kahnawake than the suitability process or its cost is the absence of many specific money laundering rules and procedures in the KGC Regulations. The bulk of the money laundering provisions are 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.”222 In other words, the 40 Recommendations—at least as they apply to Internet casinos—are imported wholesale into the KGC Regulations. A violation of any of the 40 Recommendations is therefore a violation of the KGC Regulations. Because of the breadth of the 40 Recommendations and how many other agencies seek to mimic or incorporate their terms, this may not be a bad approach.

However, difficulties exist in both principle and in practice with such an approach. While the 40 Recommendations are continually being revised and updated, the FATF devotes few resources specifically to Internet gaming and betting. The 40 Recommendations and the RBA Guidance for Casinos include Internet gaming considerations. Full-time online interactive gaming regulators, however, may be in a better position than the FATF to take the 40 Recommendations and add 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 include gaming regulators, should ensure that casinos are effectively supervised for compliance with anti-money laundering requirements. In this context, it is odd for the KGC Regulations only to mandate CPA-holder compliance with the 40 Recommendations when the 40 Recommendations provide continuing obligations with which the KGC is supposed to comply.223 By foregoing the creation of detailed local rules, the KGC may be relinquishing some of its responsibilities to its stakeholders, thereby making itself less responsive and, ultimately, less relevant as a regulatory body.

This approach may be easier to support in practice—if not conceptually—if the specific provisions in the KGC Regulations were complete. 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.”224 The KGC, however, has no such specific rules and procedures. Another provision establishes that CPA-holders must file suspicious activity reports with the KGC under cer-

---

222 Id. at § 168.
223 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.
224 Regulations Concerning Interactive Gaming, supra note 217, § 163.
tain conditions, in a form to be provided by the KGC. But the KGC has not prescribed forms for this purpose.

Other aspects of the KGC Regulations raise questions. For instance, they state 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.” It is unclear whether such 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 Kahnawake, discussed below. Also, the threshold triggering a suspicious activity report (US$5,000) and the prohibitions on withdrawals in excess of US$10,000 (absent identification) seem to be incongruent with the US$/€3,000 threshold set out in the 40 Recommendations.

Another interesting distinction is that, unlike Alderney and the Isle of Man, the KGC Regulations do not require the CPA be issued to a locally formed entity. Requiring a corporation that is licensed and regulated by gaming authorities to be set up in the licensing jurisdiction may be preferable and the best practice to ensure effective oversight. Nevertheless, regulators may control a licensee in other ways such as through supervision of its technology, the presence of a licensee’s books and records in the jurisdiction, having a local office and presence, and any number of other requirements.

Finally, this section would be incomplete without mentioning the FATF’s concerns about Kahnawake detailed in its latest mutual evaluation report on Canada from February 2008. The FATF describes the activities and organization 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.”

The FATF, however, expressed serious concerns about Kahnawake 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 gov-

---

225 Id. at § 165.
226 Id. at § 169.
227 Id. at § 165.
228 Id. at § 167(a).
230 Id. at 231.
ernments are faced with substantial challenges in determining the appropriate course of action to take concerning Internet gambling. The industry has grown rapidly and generates huge revenues. Canada must either enforce its prohibition effectively or introduce comprehensive AML/CFT regulation for the industry.231

The statement that regulation by Kahnawake is simply “not subject” to anti-money laundering regulations might be pitching the case too high. As discussed, 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 Kahnawake and FinTRAC in the context of the KGC Regulations and the 40 Recommendations has been highlighted as an area lacking clarity.

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 agencies. 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.232 Internet gaming in Malta and its licensure is governed primarily by the Lotteries and Other Games Act (the “LOGA”).233 Section 9 of the LOGA establishes that the Lotteries and Gaming Authority (the “LGA”) is charged with inquiring into the suitability of all licensees under the LOGA, ensuring that all gaming is kept free from criminal activity, and advising the Maltese Minister of Finance when creating applicable regulations.234 The main regulations regarding online gaming and betting created under the LOGA are the Remote Gaming Regulations (the “Malta Regulations”).235

The Malta Regulations provide for the issuance, suspension, and cancellation of remote gaming licences for 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

231 Id.
234 Id. at § 11(c).
235 Id. at § 11(e).
236 Id. at § 11(k).
238 Id. at §§ 7–8.
239 Id. at § 13.
8(2) of the Malta Regulations. As with Alderney and the Isle of Man, an applicant for a remote gaming licence must be incorporated under and comply with the Malta Companies Act. The Malta Regulations provide for four classes of gaming licence that encompass everything from business-to-consumer gaming and betting exchanges to business-to-business network models. At least one “key official” must be appointed by each gaming or betting licensee, who must personally supervise the operations of the licensee of which she is a key official and ensure that the licensee complies with all applicable laws and regulations, conditions of licensure, and directives issued by the LGA.

An application for any of the four classes of remote gaming licence requires remittance of a €2,330 fee. This covers the administration and investigation costs. This is a low fee and may not sufficiently cover thorough investigation costs. A separate fee is not required for key officials of each licensee. The Malta Regulations, however, permit the LGA to requisition actual investigative, inspection, and other costs from the licensee or proposed licensee “when objectively reasonable.” Interestingly, the fee schedule calls for special fees (sometimes based on an hourly rate) when the LGA must review and pre-approve a contractual relationship between a licensee and a supplier.

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 registered shareholders of the corporation, not merely those over a particular threshold percentage. The application also seeks disclosure of details concerning patents and proposed trademarks in connection with the licensed Internet gaming operations. The key official personal declaration form, however, 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”),

---

240 Id. at § 4.
241 Id. at 1st Sched. Reg. 3.
242 Id. at § 15(1).
243 Id. at § 15(2)(a).
244 Id. at § 15(2)(b).
245 Id. at 2nd Sched. Reg. 6, § 1.
246 Id. at § 6(3).
247 Id. at 2nd Sched. Reg. 6, § 5.
248 Id. at § 11(4)(e). This provision only applies when the supplier is to receive a percentage of the profits of the remote gaming operation or a commission.
the Minister of Finance may provide guidelines for gaming licensees and their employees about transactions that may raise money laundering suspicions.250 (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.251 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.252

While the foregoing provisions appear to imply that Internet gaming licensees are within the scope 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.”253 (“Subject persons” include persons carrying out relevant activities.254) In the PMLA Regulations, “casino” has the same meaning as in Malta’s Gaming Act255—and “casino licensee” is construed accordingly256—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.257 Accordingly, it is relevant to question whether or not Internet gaming licensees are specifically subject to the provisions of the PMLA and its regulations. Irrespective of any ambiguity, and given the application of the Third Directive to “casinos” in Malta, as Malta is a full EU member, local counsel and operators in Malta act like the provisions of the PMLA and the PMLA Regulations apply to Internet gaming licensees in Malta.258 Obviously, any 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, has issued a series of Implementing Procedures (the

250 Lotteries and Other Games Act (Malta), supra note 233, at § 61(1).
251 Id. at § 61(2).
252 Remote Gaming Regulations, supra note 237, at § 8(2)(g).
254 Id. at § 2(1) (definition of “subject person”).
256 Prevention of Money Laundering and Funding of Terrorism Regulations, supra note 253, at § 2(1) (definition of “casino”).
257 Gaming Act (Malta), supra note 255, at § 2 (definition of “casino”).
258 Interview with Olga Finkel, Managing Partner, WH Partners (Mar. 20, 2012).
“Malta Guidance”).259 The Malta Guidance is an attempt by the FIAU to outline the requirements and obligations of the PMLA and its Regulations and to assist in designing and implementing systems to detect and prevent money laundering and terrorist financing.260 The Malta Guidance adopts a risk-based approach at one stage,261 and requires implementation of procedures to manage the money laundering risks,262 but then expressly states that the risk-based approach itself is optional.263

The Malta Guidance mandates certain customer due diligence procedures similar to those adopted in the Isle of Man. The Isle of Man requires a B2C licensee to obtain the full name, residential address, date of birth, place of birth, and nationality of each player at account setup. 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.264 The only additional requirement is the identity reference, but customers do not need to produce documents to an online gaming licensee at this stage. When a player triggers a verification of identity threshold (for example, when a player makes 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), verification procedures include submission of valid government-issued identification documents to the gaming licensee.265 Extra due diligence is recommended with PEPs,266 and extra caution suggested in business relationships with persons from jurisdictions that are not “reputable jurisdictions.”267 The Malta Guidance also asserts that operators should pay special attention to any money laundering threat that may arise from new or developing technologies or from products that may favor anonymity.268

The Malta Guidance contains various record-keeping requirements. These include items like customer due diligence documents and details on

260 Id. at 10.
261 Id.
262 Id. at 54.
263 Id. at 57.
264 Id. at 20.
265 Id. at 20–22.
266 Id. at 50.
267 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.”
268 Malta Guidance, supra note 259, at 50.
transactions—including withdrawals and deposits—by players.\textsuperscript{269} Consistent with the rules set out by the FATF on records retention, the Malta Guidance establishes that a licensee must retain these records for no less than five years.\textsuperscript{270} The Malta Regulations mandate data retention requirements for financial reports\textsuperscript{271} and about each game played in the gaming system itself (including, inter alia, player balances, stakes played, and results).\textsuperscript{272}

Each licensee must appoint a money laundering reporting officer.\textsuperscript{273} Consistent with other reporting officer relationships, this officer must occupy a senior position within the organization where she can effectively influence the company’s anti-money laundering policy.\textsuperscript{274} The money laundering reporting officer must have a direct reporting line to the directors and have authority to act independently in carrying out her responsibilities.\textsuperscript{275} Furthermore, licensees must ensure that employees are aware of the organization’s anti-money laundering policies and train their employees to recognize and handle suspicious transactions.\textsuperscript{276} External reporting of suspicious transactions to the FIAU is provided for in subsection 15(6) of the Malta Regulations and is set out in greater detail in the Malta Guidance.\textsuperscript{277} Tipping off offenses are briefly covered in the Malta Regulations.\textsuperscript{278}

Controls over financial intermediaries working with Internet gaming operators are not specifically addressed in the Malta Guidance. (No part of the Malta Guidance is 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 some customer due diligence measures for intermediaries that licensees can rely on in certain circumstances, but it does not permit ongoing monitoring measures by another person or third party.\textsuperscript{279}

Finally, Malta maintains a series of international lists that identify various parties subject to sanctions or other restrictive measures.\textsuperscript{280}

\textsuperscript{269} Id. at 65–66.
\textsuperscript{270} Id. at 67.
\textsuperscript{271} Remote Gaming Regulations, supra note 237, at 3rd Sched., Reg. 25, § 7.
\textsuperscript{272} Id. at § 9.
\textsuperscript{273} Malta Guidance, supra note 259, at 70.
\textsuperscript{274} Id.
\textsuperscript{275} Id.
\textsuperscript{276} Id. at 82.
\textsuperscript{277} Id. at 72–75.
\textsuperscript{278} Remote Gaming Regulations, supra note 237, at § 16(1).
\textsuperscript{279} Malta Guidance, supra note 259, 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 259, at 52. Clearly such an exception does not apply to Internet gaming operators licensed by the LGA.
Nevada

The final jurisdiction in our survey is the U.S. state of Nevada. In many ways, Nevada exemplifies best practices. Nevada—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 of intra-state interactive poker only.281 Nevada’s interactive gaming regulations allow for three basic types of licence: an interactive gaming operator licence;282 a licence to manufacture interactive gaming systems;283 and, a service provider licence.284

The process for determining suitability in Nevada is impressive and expensive. The initial licence fee for an establishment to operate interactive gaming is US$500,000.285 The inquiries and investigations made by the state Gaming Control Board (the “GCB”) are extensive and the burden of proof is at all times on the applicant.286 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.”287 Investigations do not begin unless and until the estimated investigation fees are paid.288 Historically, every shareholder of a private corporation applying for a non-restricted licence in Nevada had to be found suitable by the GCB. Recent amendments to the Nevada Gaming Control Act and attendant regulations, however, 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.289 Persons applying for registration, however, still must complete extensive applications. That said, whether a corporation seeking a non-restricted licence is publicly traded or not, the GCB can require any person holding any beneficial interest in the licensee to undergo a full finding of suitability.290

281 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”).
284 Nev. Gaming Comm’n. Reg. 5.240(2)(d) and Reg. 5.240(3).
288 Id.
The investigation is thorough. Disclosure through the Multi-Jurisdictional Personal History Disclosure Form, for example, touches on everything 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.\(^ {291} \) Anecdotes about the bizarre things arising in investigations are legion. For example, one story involves a team of gaming control agents flying to the east coast of the U.S., auditing a safe deposit box of a license applicant at a bank, and discovering US$25,000 labelled “payoff funds.”\(^ {292} \)

An application for licensure as an operator of interactive gaming in Nevada will be made, processed, and determined in the same manner as a non-restricted gaming licence application.\(^ {293} \) The same high (non-restricted gaming licence) standard applies to a licence applicant for becoming a manufacturer or distributor of an interactive gaming system\(^ {294} \) 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).\(^ {295} \)

Anti-money laundering mandates and rules in Nevada come from two primary sources: the federal Bank Secrecy Act of 1970 (the BSA)\(^ {296} \)—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”).\(^ {297} \)

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 the Indian Gaming Regulatory Act (other than an operation limited to class I gaming).\(^ {298} \) 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;\(^ {299} \)

\(^{291}\) Cabot & Kelly, supra note 2, at 137.

\(^{292}\) Id.


2. Report any suspicious transactions, and make sure that no person involved in the transaction is notified that the transaction has been reported (tipping-off).

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,” and,

4. Consult lists of known or suspected terrorists (e.g., the OFAC’s Specialy Designated Nationals List) to determine if anyone seeking to open an account appears on such a list.

The Nevada Regulations require operators to implement procedures 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. In other words, Nevada law compels compliance with its own money laundering prevention system, the BSA, and other statutes. This broad mandate is given specific effect throughout the Nevada Regulations.

One example of this specificity is the customer due diligence performed during player registration. At the creation of a player’s authorized interactive gaming account, the Nevada Regulations set out information that interactive gaming operators must collect. This information includes the player’s name, the physical address where the player resides, his or her date of birth, and the player’s social security number (if a U.S. resident). It also includes confirmation that the player has not been previously self-excluded and is not on the Nevada blacklist. Unlike other jurisdictions examined here, Nevada requires, within thirty days of providing registration information, that the interactive gaming operator must perform procedures to verify the information and that the operator must limit the player’s gaming activity during that verification period. The player, however, may not deposit more than US$5,000 into her account during the verification period, which is a high threshold. All the same, the player cannot withdraw funds during the verification period, which is a good check to have in place. The verification procedures must be recorded and maintained, and the MICS suggest that the licensee obtain and record credentials from the

---

300 31 U.S.C. § 5318(g).
player and record and verify the date of birth and physical address from external sources.313 If the verification has not occurred within thirty days, the operator must immediately suspend the interactive gaming account.314

Some parallel identification requirements exist between the BSA and Nevada’s regulations; for example, when a report on a transaction amount exceeds US$10,000, operators need to file the appropriate reports. The items to be verified and recorded include name, account number, and social security number or taxpayer identification number (if any).315 For non-residents or aliens, verification of identity “must be made by passport, alien identification card, or other official document evidencing nationality or residence.”316

Robust provisions exist for transfers of amounts between an interactive gaming account and the same player’s land-based casino account.317 Furthermore, when a player makes an in-person withdrawal request at a bricks and mortar gaming establishment (after transferring from her interactive gaming account), casinos must record certain particulars and the player must sign for the withdrawal.318 The player must present identification for the withdrawal at the casino.

Authorized gaming players may hold only one interactive gaming account with an operator;319 anonymous interactive gaming accounts or accounts in fictitious names are prohibited.320 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.321 Transfers from one authorized player to another authorized player are not permitted (except for wins and losses at the virtual poker tables).322

Besides the suspicious activity reports required under federal law, the Nevada Regulations contain their own provisions for reporting “suspicious wagering” when the wager is suspected of being in violation of federal or state law323 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.”324

316 Id.
On records retention, Regulation 5A.190 states that operators must maintain “complete and accurate records of all matters related to their interactive gaming activity,” including player identities, player registration, and complete game histories for every game played on the interactive gaming system.\textsuperscript{325} Consistent with the FATF standard, operators must preserve these records for at least five years after they are made.\textsuperscript{326}

Finally, regarding payment processing intermediaries, 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 non-restricted licence applicant) or as a Class 2 service provider (i.e., only required to make a restricted licence application), depending upon the nature of the relationship with the operator and the intermediary’s relationship to the flow of funds between operator and customer. Irrespective of how such intermediaries are licensed, however, Nevada takes a strong interest in evaluating and monitoring the payment processors used by operators. For example, section 82 of the MICS requires that the interactive gaming operator’s internal control standards delineate: procedures established for the use of each payment processor,\textsuperscript{327} all deposit methods available to authorized players, and a complete description of the entire process for each method.\textsuperscript{328}

Nevada has consulted widely and adopted the 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.

**Thoughts on Best Practices**

Given the breadth of the FATF’s recommendations—and the depth and expertise of the FATF itself—many best practices reflect the 40 Recommendations. The suggested best practices for currency and transaction handling and prevention of money laundering in online gaming are as follows:

1. Regulating the sector;
2. Adopting a dynamic, risk-based approach;
3. Transparency of all participants;
4. Traceability of all transactions; and,
5. Control of operators by regulators and security of their operations.

Almost any set of systems will generate overlap. For example, regulation strongly implies assessments of suitability, but suitability assessments

---

\textsuperscript{325} Nev. Gaming Comm’n. Reg. 5A.190 (2011).
\textsuperscript{326} Id. 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.
\textsuperscript{327} Nev. Gaming Comm’n. Minimum Internal Control Standards § 82(a) (2012).
\textsuperscript{328} Nev. Gaming Comm’n. Minimum Internal Control Standards § 82(b) (2012).
are covered under the heading 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 funds is acknowledged.) This taxonomy tries to keep the groupings as discrete as possible.

**Internet Gaming Should be Regulated**

The best practices for regulation assume regulation. Whether the industry should be regulated at all, however, is not universally agreed. Many continue to believe that Internet gaming should be banned outright or ignored by policy makers. For example, many states in the US and provinces in Canada with land-based casinos 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. From an anti-money laundering standpoint only, the need for regulation of the industry is obvious. Simple prohibition increases the chances for money laundering; regulation cuts against it. Regulators, however, must have appropriate funding to properly undertake their work. Regulation of the industry requires continuing resources and commitment by policy makers.

Recommendation 28 in the 40 Recommendations establishes that Internet casinos “should be subject to a comprehensive regulatory and supervisory regime” that ensures they have effectively implemented the necessary components of the 40 Recommendations. Minimum requirements include having competent authorities to license Internet casino operators. The rationale for this approach ranges from the preservation of freedom to undertake (what some find to be) objectionable activities, while minimizing or “managing down” collateral harms, to the futility of trying to prohibit those activities.

From the perspective of preventing money laundering, the case for regulation of the Internet gaming sector is strong. According to Cabot and Kelly, most experts agree 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.”

---


330 Id.

331 See, e.g. Levi, supra note 8, at 26.


333 Cabot & Kelly, supra note 2, at 136.
ing in an online context and, in fact, the authors go on to note the negative relationship between strong Internet gaming regulation and money laundering opportunities. The other thing to note from Cabot and Kelly is that the role for regulators transcends suitability assessments; suitability is a necessary, but not sufficient, precondition for preventing money laundering.

Regulation suggests that a blanket prohibition will not work, even if prohibition 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”). 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 in transferring funds to online gambling websites. (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.”) 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. For good measure, one might have added that these alternative processes might also be illegal. Poor regulatory oversight, among other things, helps money laundering thrive.

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.” Regulators also must have stable and sufficient funding for their activities and operations. Without proper resources, a great regulatory framework may be completely ineffective.

334 Id. at 144–145.
335 See also id. at 139: “Admittedly, the problem of money laundering may still remain notwithstanding the suitability of gaming operators.”
336 H.R. 556, supra note 46.
338 Schwartz, supra note 48, at 128. See also Koenig, supra note 332, at 36–37.
340 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).
341 Valasek, supra note 337, at 765.
342 Cabot & Kelly, supra note 2, at 137–138 (discussing the effects of a lack of resources in various quarters on land-based casino gaming regulation in New Jersey).
343 See supra text accompanying note 210.
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. 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 in section 6.) Internet gaming regulators should consider whether any particular MVTS are regulated and assess the quality of that regulation. Regulators and operators should prefer more regulated and reputable MVTS businesses rather than less regulated and less reputable solutions.

Adopt a Dynamic, Risk-Based Approach

Regulators should implement a risk-based approach dynamic and flexible enough to adapt to changing circumstances. This is imperative in an industry 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.” It means that, besides minimum thresholds subject to constant refinement, states, regulators, and operators should deploy their resources where they will have the most impact and away from areas of comparatively little concern.

Why adopt a risk-based approach? Would an accounting audit checkbox 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 in the nature of electronic commerce itself. Money laundering threats change constantly and vary across customers, jurisdictions, products, delivery channels, and over time. 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 penetration might offer more anonymous payment options already present in a mobile market and that may have been initially intended 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; a prescriptive, static check-box standard would likely be off-target and not deliver benefits greater than the costs of intervention and regulation. As one author succinctly puts it, the online interactive gaming business is a “stunning example of technology outpacing the law.”

---


345 Id.

346 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
and rational to address existing threats and it must be flexible enough 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 favor anonymity or that otherwise challenge or undercut effective anti-money laundering procedures with caution.

The risk-based approach advocated here is the same as that adopted in the 40 Recommendations (see section 4). 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 adopted measures intended 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.”

Two attributes of a risk-based approach are critical. The first is that the concept of risk is not subjective or defined by one person or institution. While room for debate exists to determine whether certain industries pose higher or lower risks, 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 apparent that large and anonymous cash transactions are higher-risk than traceable transactions through a reputable and licensed bank.

The second attribute is that a risk-based approach does not mean the absence of minimum objective standards. Indeed, the first of the 40 Recommendations mandates a risk-based approach, but the remaining 39 recommendations require a comprehensive framework for addressing minimum standards to deter 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 change 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 more of the best possible practices. Collectively, at least some of these thresholds form a floor on anti-money laundering standards in Internet gaming. In the next section, this chapter presents 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

detecting the money laundry cycle is the vast amount of resources that traffickers can devote to innovating money laundering techniques.” Bachus, supra note 2, at 845–846.

Regulating Internet Gaming

reported. In the section on the traceability of transactions, the chapter recommends that regulators must be wary of allowing cash to be accepted by any intermediary between the Internet gaming operator and the customer, at least without the intermediary undertaking robust due diligence, 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, however, can present some challenges. 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. Accordingly, a risk-based approach demands a better trained, more expert, and therefore more expensive staff. 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.

With all of its challenges, however, the risk-based approach is the best approach to prevent money laundering and is clearly the dominant one. When layered on top of minimum standards and procedures, and where a regulator is properly structured and funded, any concerns about it can be effectively addressed. Increased analysis can lead to better protocols and decisions. Increased and targeted resources in an anti-money laundering context should have beneficial effects. The FATF sets out several specific transaction risk issues raised by Internet casinos. These include multiple accounts, changes to financial institution accounts, and the use of prepaid cards and electronic wallets.

A dynamic risk-based approach is a best practice for Internet gaming regulation; this does not mean 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.

All Participants Should be Transparent

In certain key respects, phrases like transparency, know your client, due diligence, identification and verification procedures, etc., are shorthand for understanding one’s customers and business partners. With transparency, a mix of minimum standards and a risk-based approach is at play.

Transparency into regulatory, business, and customer relationships begins with suitability assessments by regulators. In this area, of the surveyed jurisdictions, Nevada has a commendable approach. It has a com-

348 Id. at 8–9.
349 Id. at 27–28.
350 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.
prehensive system 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 with the prospective licensee or associated with the licensee. The costs and the investigation of staff demonstrate that Nevada regulators take the process very seriously, which is appropriate from an anti-money laundering standpoint alone. As noted, being careful about who is regulated is a starting, critical bulwark against money laundering. No magic number defines how much regulators should charge to investigate applicants and their respective associates, but it must be enough to fund meaningful and relevant inquiries.

The next stage is assessment of the operator’s customers and business partners. In the latter case, regulators should license some of these parties as service providers. Beyond licensure, however, regulators should mandate that Internet gaming operators implement checks and procedures to evaluate 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 paramount importance are the internal and external procedures followed by the business partners who deal with their own customers or the customers of the licensee on the licensee’s behalf.

The positions of MVTS or other financial intermediaries are of utmost concern because they process payments for Internet gaming licensees. Here, a risk-based approach must be taken. Banks in well regulated and respected jurisdictions should be perceived as low-risk; debit and credit cards issued by such institutions and used to fund customer accounts should be seen, accordingly, as a reduced risk. Beyond that, operators should use caution when selecting MVTS partners, although a service like PayPal is relatively low-risk. PayPal is an electronic wallet regulated as a money services business in the United States. Upon registering and funding a PayPal account, one must link to an already-issued credit card or bank account, meaning that PayPal itself interfaces with trusted institutions in the financial system.

Internet gaming operators should approach any MVTS business or intermediary who accepts cash on an anonymous basis with great caution. This warning does not include banks and other financial institutions that perform 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 become suitable intermediaries provided that they collect and maintain satisfactory player due diligence and, crucially, that they maintain comparatively low thresholds on the amount a customer can deposit on a card or voucher (i.e., these would need to be below the US$/€3,000 withdrawal threshold in place in the 40 Recommendations).
As to customer due diligence in a B2C gaming operation, procedures in Nevada and the Isle of Man are suitable. Measures need to comply with FATF recommendation 10. Minimal information may be acceptable at the customer registration stage, and such information need not necessarily be checked against an external database. (That said, the Nevada example of requiring a verification check when registering every player is a standard to which all regulators should aspire.) However, the US$/$€3,000 threshold should trigger enhanced customer due diligence procedures accompanied by attempts to verify the customer’s identity with government-issued documents, and requiring direct customer contact. In addition, the risk-based procedures of a regulated company like Paddy Power demonstrate the best practices in this category. They 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). 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 for dealing with certain customers, there are some players who operators should refuse to service. It is in their—and the public’s—best interest to respect the Specially Designated Nationals List maintained by OFAC and to decline to engage in a business relationship of any kind with listed persons. They also need to implement measures that use private or alternate databases to prevent circumvention of this requirement by those listed.

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 or other sources. Regulators may augment such a database with their own investigative or monitoring findings, as appropriate. Transparency is key to the best practice for regulators; its essence is knowing with whom one is dealing. It extends from assessments of suitability by the regulator to risk-based assessments, minimum due diligence and investigation standards.

351 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 chapter.

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 offenses that have already occurred.

Regulators and operators must determine the financial choke points of criminal activity. Choke points are entryways and exits through which funds must pass as they are disseminated throughout the economy.353 These choke points are opportunities to record transactions and customer identities, “thereby creating a ‘paper trail’ that law enforcement can use to trace laundered funds from which they were originally derived.”354 Placing a transaction on a credit card, depositing money to a PayPal e-wallet, and withdrawing funds from a bank are examples of instruments passing through a choke point in the system. Many money launderers seek to circumvent these choke points, which is why large cash transactions and anonymous cards that contain electronic money can cause concern. The best anti-money laundering practices must try to, as much as possible, guide consumers, business partners, and transactions through functioning and reliable choke points in the financial system. Accordingly, the Isle of Man prohibits licensees from accepting cash from customers and business participants. Where there is a parallel bricks and mortar and interactive structure, as in Nevada, rules similar to the Nevada Regulations address transfers between land-based and Internet channels.

Operators need to remain diligent and question the sources of funds of a business partner or a customer. The origin of any party’s funds and establishing the identity of that party is a crucial check on their ability to launder funds through an Internet gaming business. Both bulwarks are important and related, but 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. 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—operators must make inquiries 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. Operators should employ similar rules when Internet gaming licensees establish business relationships with suppliers and customers.

353 Rueda, supra note 2, at 9.
354 Id.
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 with PEPs. It seems only fair that most PEPs should not automatically be denied Internet gaming or business relationships, if desired by all parties, but particular care must be taken to ensure that the relationship does not advance corruption in the PEP’s home jurisdiction, for example.\textsuperscript{355}

Another situation that requires determination of sources of funds is when the business partner or customer of the Internet gaming licensee 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.\textsuperscript{356} Here again, nationals or other parties hailing from those countries should not automatically be shut out of business relationships entirely, but a higher degree of scrutiny should apply. With recommendation 29, enhanced due diligence with principals from these various jurisdictions is mandatory, but requiring an investigation of the sources of funds from these countries may be perceived as going beyond the current scope of the 40 Recommendations.

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. 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):

- Information and copies of documents obtained in any customer or business partner due diligence process;
- Information obtained through the risk assessment process and review relating to any customer or business partner;
- The results of all inquiries into and investigations of any customer or business partner;
- Full financial details, including wiring information and financial intermediary information, of every deposit and withdrawal made by each customer; and,
- The full records of each game or bet played by each customer, including the stakes brought to the table, the cards played with results of each hand, and funds won or lost.\textsuperscript{357}

\textsuperscript{355} A PEP’s relationship with the Internet gaming operator should be subject to enhanced ongoing monitoring, as well.

\textsuperscript{356} 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 http://www.fatf-gafi.org/document/18/0,3746,en_32250379_32236992_49694738_1_1_1_1,00.html.

\textsuperscript{357} This five-year requirement is without prejudice to any additional requirements that may
Copies of these records should be kept when produced to regulators or to law enforcement, unless it breaches applicable law. An Internet gaming operator’s regulator should receive everything it requests; regulators are entitled to this information. Unless otherwise prohibited, when the local FIU or other law enforcement requests assistance, regulators should be notified and operators must comply. Regulators should mandate co-operation with international financial crime authorities and other investigators with authority, provided that such co-operation does not conflict with an operator’s regulatory obligations.

Finally, operators should implement suspicious transaction reports and the money laundering reporting officer usually coordinates these reports. Based on the risk-based approach, it is possible that operators must make a report to law enforcement even if there is no financial transaction with an Internet gaming licensee, for example, when a new customer’s identity cannot be sufficiently verified or when operators refuse a large transaction.

Sound traceability principles require an effort to push Internet gaming and betting transactions through legitimate and effective choke points. This implies prohibiting licensees from accepting cash. Impeccable record-keeping and reporting standards are a must, and should complete any good approach when tracking the flow of funds through a regulated gaming environment.

**Regulators Need to Control the Gaming Environment and Foster Security**

Best practices include some form of broad control to secure multiple parts of the gaming structure. It protects access to data and encompasses 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 to support other preferred practices, it also includes appointing a suitably-empowered money laundering reporting officer. Finally, it is imperative to guard the confidentiality of investigations and prevent tipping-off.

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 presence in the licensing jurisdiction with which regulators are familiar. It also, in a sense, forces the applicant to “commit” to the jurisdiction, although this commitment takes several forms, including completion of the application, paying the application fee, and disclosures. Moreover, the local corporation requirement means that regulators have a greater level of control over
the licensee. Applicable corporate law may require a corporation to have its books and records or offices in the country, pay local taxes, and have technology in line with the local regulating jurisdiction. These become instruments that a regulator can reach out and influence in order to bring a recalcitrant licensee into line, if necessary. It is also administratively easier for a regulator to coordinate with other local authorities to discipline an Internet gaming licensee. For this reason, local corporation nexus is always preferable when establishing the 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 licensee. 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 for Internet gaming regulators to have control over the licensee, at least in principle. Gaming regulators can mandate that there be a local corporate, technology, physical office, or other presence whether a corporation hails 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 regulators have sufficient control of Internet gaming licensees.

In an anti-money laundering context, regulators must be able to reasonably and quickly access any required records in an acceptable form. As important, Internet gaming regulators must have effective control over who has access to those records. This provides a trail for regulators to know how records have been accessed or modified and to prevent data corruption, thus supporting the data retention recommendation. It also serves as a warranty to the betting public that its licensees 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 international character. While the money laundering reporting officer works for the licensee, sufficient independence can be written into relevant rules and procedures to ensure that she can attain a higher level 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 co-ordinate staff with anti-money laundering training and procedures.

Finally, as an adjunct to data protection and preserving the integrity of
any investigation by either the licensee, the regulator, or law enforcement, rules that prohibit tipping-off must be implemented. Suitable penalties for breach of tipping-off rules need to be in place. These regulations should extend to anyone who has knowledge of a relevant investigative process or with anyone who has a duty to report suspected activity in the organization. Because the group of people who have a duty to report money laundering suspicions to the appropriate authorities is potentially large, those subject to tipping-off restrictions are also numerous. This recommendation should be backed up by protections for good-faith disclosures by any employees or agents.

Sufficient control of licensees and securing the Internet gaming regulation and operational structure is essential. Local corporate requirements are desirable but may not be essential in all cases. Regulators must have access to and control over availability of data logs and records. Operators need to appoint a suitably trained and higher ranking money laundering officer and provide relevant training to staff. It is also imperative that operators implement tipping-off and confidentiality measures that regulators monitor.

Selected Payment Intermediary Issues

A comparison of two e-commerce payment intermediaries within the best practices framework demonstrates the strengths and weaknesses of each. 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 in the news of late. PayPal meets the various applicable tests for being a low-risk and usable payment mechanism. Bitcoin causes more concern.

PayPal

As discussed previously, PayPal is an electronic wallet that has been variously described as “a peer-to-peer payment system”358 and “not electronic money per se” but an approximation of the use of e-money.359 PayPal was launched in 1999.360 PayPal initially processed Internet gaming charges but agreed to cease doing so in 2002 upon its acquisition by eBay.361 PayPal is a system that allows its customers to deposit into e-wallets, i.e., accounts maintained on the PayPal system that shows credits (liabilities) to PayPal’s customers, with cash held as the corresponding debits (assets). (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

358 Ormand, supra note 339, at 452.
359 Schopper, supra note 2, at 318.
360 Id.
361 Ormand, supra note 339, at 452.
## Table 2

**Best Practices Summary for Internet Gaming Regulators**

<table>
<thead>
<tr>
<th>No.</th>
<th>Best Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Regulation</strong></td>
</tr>
<tr>
<td></td>
<td>• Establish suitable rules, procedures, and institutions to regulate Internet gaming and ancillary activity.</td>
</tr>
<tr>
<td></td>
<td>• Regulation must be robust and continuing.</td>
</tr>
<tr>
<td></td>
<td>• Regulators must have sufficient resources to do their jobs.</td>
</tr>
<tr>
<td>2</td>
<td><strong>Risk-Based Approach</strong></td>
</tr>
<tr>
<td></td>
<td>• Assessing risk should be in accordance with international norms and standards.</td>
</tr>
<tr>
<td></td>
<td>• Must be dynamic and flexible in order to address new risks; reject overly mechanical approaches.</td>
</tr>
<tr>
<td></td>
<td>• Minimum standards still apply, which are also subject to constant refinement.</td>
</tr>
<tr>
<td></td>
<td>• Pay particular attention to new technologies, especially new technologies that favor anonymity or otherwise undercut effective anti-money laundering procedures.</td>
</tr>
<tr>
<td>3</td>
<td><strong>Transparency</strong></td>
</tr>
<tr>
<td></td>
<td>• Regulators must fully inquire into prospective licensees and their associates; the cost of licensure must be commensurate with a high standard.</td>
</tr>
<tr>
<td></td>
<td>• Regulated MVTS and financial intermediaries should be favored over unregulated parties; intermediaries accepting cash should be approached with caution.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Each player may have only one gaming account per operator.</td>
</tr>
<tr>
<td></td>
<td>• Transactions and business with certain parties (e.g., on the OFAC list) should be prohibited outright.</td>
</tr>
<tr>
<td>4</td>
<td><strong>Traceability</strong></td>
</tr>
<tr>
<td></td>
<td>• Customers, business partners, and transactions should be funnelled through financial choke points; Internet gaming operators should never accept cash from customers or business partners.</td>
</tr>
<tr>
<td></td>
<td>• 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.</td>
</tr>
<tr>
<td></td>
<td>• Suitable record-keeping and suspicious transaction reporting standards are required for traceability.</td>
</tr>
<tr>
<td>5</td>
<td><strong>Control &amp; Security</strong></td>
</tr>
<tr>
<td></td>
<td>• Strongly prefer licensees to be locally-incorporated. In any event, ensure that regulators have sufficient levers to control and discipline its licensees.</td>
</tr>
<tr>
<td></td>
<td>• Regulators must have timely access to relevant records and be able to control access to those records.</td>
</tr>
<tr>
<td></td>
<td>• A suitably trained and independent money laundering reporting officer must be appointed; other staff in the organization must receive anti-money laundering training.</td>
</tr>
<tr>
<td></td>
<td>• Tipping-off should be prohibited and good-faith disclosures about suspected money laundering should be protected within the bounds of applicable law.</td>
</tr>
</tbody>
</table>
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.\textsuperscript{362}

The success of PayPal should not cause any particular concern to those seeking to suppress money laundering within Internet gaming. PayPal is currently available as an e-wallet for use on Internet gaming sites in more heavily regulated markets. More important, PayPal is itself regulated in the United States, for example, offering 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 is licensed in a majority of U.S. states.\textsuperscript{363}

The procedure for depositing into one’s PayPal account is 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. This mixture of regulation as a MVTS provider 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.

**Bitcoin**

By contrast, Bitcoin is an electronic payment system that has received a great deal of recent attention and generated controversy. Bitcoin the payment system should not be confused with bitcoin the currency. 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,” or team of coders, and certainly an alias) in January 2009.\textsuperscript{364} This non-fiat currency is controlled entirely by software. A total of 21 million bitcoins are scheduled for release through this software, almost all of them over the coming 20 years.\textsuperscript{365} Every ten minutes, coins are dis-

\textsuperscript{362} On the factors favouring a move away from credit cards towards electronic wallets and other payment systems (including PayPal), see generally Rueda, supra note 2, at 29–36.


\textsuperscript{365} Id.
tributed through a process resembling a lottery. Bitcoin “miners” play this lottery over and over; the fastest computers employed by miners win the most bitcoins released by the software.

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). More recently, bitcoins have reached prices in excess of $220. There are several Internet betting and gaming websites—including sealswithclubs.eu, btcsportsbet.com, and satoshidice.com—operating exclusively using bitcoins. Other sites offer Bitcoin as a payment mechanism.

According to its inventor(s), bitcoin was developed to address “the inherent weaknesses of the trust based model” of electronic commerce. Central banks must be trusted not to debase a currency; retail, commercial, and other banks must be trusted to safeguard money on behalf of customers. In the estimation of Bitcoin’s inventor, history is littered with evidence of breaches of that trust. 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). With bitcoins, transactions are non-reversible and, through encryption of each transaction, does not permit the same bitcoin to be spent more than once (eliminating fraud).

The critical aspect of bitcoin 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.” Nakamoto states 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.”

366 Id.
367 Id.
368 Id.
371 Id.
372 Bitcoin Design Paper, supra note 369, at 1.
373 Davis, supra note 364, at 65.
374 Bitcoin Design Paper, supra note 369, 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.
How easily can the parties to a bitcoin transaction be identified by law enforcement? One organization that examined bitcoin calls the anonymity in the payment system “complicated”\textsuperscript{375} 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.”\textsuperscript{376} An apparent member of the Bitcoin development team has been quoted as follows: “Attempted major illicit transactions with bitcoin, given existing statistical analysis techniques deployed in the field by law enforcement, is pretty damned dumb.”\textsuperscript{377}

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 methods to obtain this information for regulators or law enforcement should be necessary in a well-regulated Internet gaming environment. It appears 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,”\textsuperscript{378} 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 currency or a payment system 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 chapter. Attempts to reduce fraud by not allowing the same virtual money to be spent twice are commendable, 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 these matters 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.

\textsuperscript{376} Id. at 12.  
\textsuperscript{378} Davis, supra note 364, at 70.
Conclusion

This chapter examined money laundering and why it matters. The constraints and limitations on this analysis have been acknowledged and explored. The FATF’s 40 Recommendations and the anti-money laundering rules and procedures in Alderney, the Isle of Man, Kahnawake, Malta, and Nevada have been examined. Based on the comparatives available, we have set forth some thoughts on five best key 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 discussion like this is always part of a broader puzzle. It is not the definitive comment on the subject. In an industry as young, dynamic, and subject to technological change as Internet gaming, a ‘last word’ in a book chapter is 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 tool to encourage more detailed discussion among regulators, operators, and law enforcement.