UNLV
International Center for GAMING REGULATION

Online Casinos, Alternative Payment Mechanisms and the Associated Financial Crime Risks

Prepared by Amanda Gore
February 2022

Acronyms and abbreviations

Abbreviation	Meaning
AGCC	Alderney Gaming Control Commission
AML/CFT	Anti-Money Laundering/Countering the Financing of Terrorism
AMLC	Anti-Money Laundering Council (Philippines)
APG	Asia-Pacific Group on Money Laundering
BSA	Bank Secrecy Act (US)
CBDG	Central Bank Digital Currency
CVC	Convertible Virtual Currency
CDD/KYC	Customer Due Diligence /Know Your Customer
DNFBP	Designated Non-Financial Businesses and Professions
FINCEN	Financial Crimes Enforcement Network
FIU	Financial Intelligence Unit
FSRC	Financial Services Regulatory Commission (Antigua)
IOM	Isle of Man
MSB	Money Services Bureau
NFT	Non-Fungible Token
PAGCOR	The Philippine Amusement and Gaming Corporation
PEP	Politically Exposed Person
POGO	Philippines Offshore Gaming Operator
STR/SAR	Suspicious Transaction Report /Suspicious Activity Report
UIGEA	Unlawful Internet Gambling Enforcement Act
USD	United States Dollar
VC	Non-convertible virtual currency
VIP	Very Important Person
VPN	Virtual Private Network

Acknowledgements

This research has benefited from the review and advice by a number of key experts in the industry to which we express thanks and gratitude. The author wishes to thank to the University of Nevada, Las Vegas ("UNLV") International Centre for Gaming Regulation ("ICGR") for its support to develop this paper under the 2021 research fellowship.

Executive Summary

The report seeks to understand the evolution of both online gambling operations and the associated alternative payment methods that support online gambling activities. Online gambling is defined as "*betting on games of chance"* over the internet and includes casino slots, sports betting, horse betting, card games along with e-games.[1] Technological advancement has supported the development of an infrastructure to support online gambling activities with live game play and dealers, blurring the line between land-based and online casino offerings. The ease of downloading apps has also expedited the proliferation of game play and online gambling globally. Online payment systems have also evolved from supporting traditional e-commerce to including a range of payments available for gambling clientele such as cryptocurrencies, traditional payments including banks, mobile money transfers, prepaid/stored value cards, and e-wallet services.

The first section of the report will document the rise of online gambling and critically examine alternative payment methods and third-party payment providers that facilitate online payment between gamblers and the online casinos. The final sections of the report will examine the regulatory landscape with a focus on any potential gaps that need to be addressed. Case studies are also presented based on law enforcement actions and/or interviews that reveal information linked to financial crime issues.

Key Findings:

> The level of regulation for online casinos varies greatly from jurisdiction to jurisdiction with some highly regulated and reputable locations for online operators.
> Gambling regulators have a range of enforcement tools and administrative sanctions they can apply to non-compliant operators.
> Multiple government agencies play a role in overseeing online casinos including the financial regulator, the financial intelligence unit, the police (to combat illegal gambling operators) and the tax agency.
> Alternative (non-traditional) payment systems are commonly used by online gambling operators and are often endorsed by gaming regulators if the payment service is itself regulated.
> Emerging trends include the rise of social gaming and crypto casinos.

The purpose of this paper is to compare and contrast regulatory practices across a range of jurisdictions that supervise online gambling with a key focus on reviewing AML/CFT procedures and identifying potential risk areas. Finally, high-level guidance on best practice regulation to manage AML/CFT risks that may be associated with online gambling are offered.

[1] Online gambling can also be referred to as internet gambling or i-gaming. E-gaming can refer to online video games and slot machines for example.

Methodology

This research has relied upon an extensive review of available policies and procedures for online operators and their associated AML requirements in selected jurisdictions that regulate online casino operations. This policy review has been supplemented with open-source research, interviews with gaming oversight agencies and industry experts along with conducting live "walk-through" scenarios with randomly selected online casinos to review payment methods available and to identify potential AML risks. The research has benefitted from expertise, advise and documentation from the following jurisdictions: Alderney, the Philippines, Antigua and Barbuda, the Isle of Man, Curacao, and Costa Rica. It also touches on Malta and Gibraltar as prominent gaming destinations.

For purposes of this paper, the term "gambling" refers to casino gaming, betting, poker, lotteries, bingo, whereas "gaming" refers only to casino games.

Section 1: The rise of online casinos & alternative payments

The online gambling market has been growing at a phenomenal rate and is expected to reach USD 100 billion in 2026, up from US 50 billion in 2019.[2] Other expert reports are more optimistic and suggest that the market may reach 93 billion by 2023.[3] The regulation of online gaming covers *"betting on any game of chance"* and usually includes online casino games like slot machines, poker, roulette, card games, sports betting facilities and in some cases e-gaming. The growth of this market has accelerated due to the accessibility of the online platforms through mobile apps and enhanced functionality due to advances in technology. Online gambling has also grown exponentially in the last two years with more demand for entertainment options at home opposed to in-person socialising due to the COVID-19 pandemic. The development and advancement in internet payment technologies have also assisted in supporting the online casino market with the rise in the number of third-party payment providers, e-wallets, and payment providers to support online transactions and in-app purchases.

The online gambling industry first evolved in the 1990s when technology developed to create online shopfronts and e-commerce markets. With the acceleration of internet speeds, the capability to stream video and integrate payment platforms became more commonplace and online casinos began to take shape. These advances in technology have helped to facilitate higher quality online games, slot machines, and include live dealers which can essentially replicate the same experience for a gambler as land-based casinos. With the introduction of mobile apps, the proliferation of betting online and joining online casinos has become available to mass markets. Online gaming and the rise of social gaming has also been "changing the game" as crypto casinos and non-fungible tokens (NFT) games become more popular. Revenue in the online e-games segment is projected to reach US$26,290m in 2022. "*Online games are defined as massive multiplayer online games (MMOGs) as well as casual and social games that can be either played directly in an internet browser or via clients that need to be installed."*[4]

[2] Facts and Factors https://www.fnfresearch.com/online-gambling-betting-market-by-game-form-type
[3] Statista https://www.statista.com/statistics/270728/market-volume-of-online-gaming-worldwide/
[4] Statista https://www.statista.com/outlook/dmo/digital-media/video-games/online-games/worldwide

The history of law enforcement actions against online gambling operators

With such significant growth for online gambling and a lack of clear laws and regulations, it was inevitable that law enforcement would be curious about these new and very profitable businesses. On 15 April 2011, the Department of Justice (DOJ) shut down multiple online poker sites that were previously accessible to US players including PokerStars, Full Tilt Poker and Absolute Poker, a date now known as Black Friday. The charges focused on fraud and online operators utilising the US banking system to facilitate (illegal) gambling activity. Further indictments were issued for online casino operators in this period leveraging money laundering laws to further the charges. This curious link between online casinos and the associated money flows has been a key feature of the establishment of the industry especially linked to US markets. US law linked to online gambling has not always been clear. The US Government had initially argued that online gambling was a violation of the Wire Act 1961[5] and later the Unlawful Internet Gambling Enforcement Act ("UIGEA")[6] when it passed in October 2006. However, more recent court rulings in 2019 and 2021 have reaffirmed that the Wire Act applied to gambling activities on sporting events and does not prevent online casino gambling (I-gaming) or online lotteries.[7][8] It is believed that between 2013-2018 more enforcement action of casinos took place than the prior 20 years.[9] Full Tilt Poker was indicted in 2011 through one of its founders, Ray Bitar, and head of payment processing, Nelson Burtnick. The allegations included unlawful gambling, conspiracy to defraud banks, wire fraud, and money laundering conspiracy. The essence of the allegation was that Bitar and Burtnick tried to circumvent US restrictions on gambling and used the US banking system as part of their internet gambling business. This allegedly involved the miscoding of credit card transactions and setting up phony companies to ensure banking services (merchant accounts) were extended in the US to take the deposits of US gamblers, contrary to US law. *The US Attorney in New York also suggested that the companies, along with their payment processors, had tried to circumvent the UIGEA by disguising gambling revenues as payments for jewellery, golf balls and various other sports paraphernalia.*[10]

As one of the first jurisdictions to regulate online casinos, Antigua and Barbuda ("Antigua") were also caught up in several US law enforcement actions. Antigua began licencing online casinos in the mid-90s and at its peak licenced hundreds of online casinos before a combination of higher taxes and US law enforcement actions saw a decline in registration. There are now a number of jurisdictions competing for the income derived from licensing online casinos, the most well-known include: The Isle of Man, Malta, Gibraltar, Curacao, Alderney (Guernsey), Kahnawake (Canada), Costa Rica, New Jersey (USA), Denmark, Italy, Estonia, Spain, Sweden

[5] The Wire Act, 18 U.S.C. Section 1084, was enacted in 1961 to assist states in enforcing their gaming laws and to suppress organized gambling activities across state lines. The statute contains two provisions. The first prohibits anyone in the business of betting or wagering from knowingly using interstate communications to transmit "bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest" and the second prohibits "the transmission of a wire communication entitling the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers." (Source: https://www.lexology.com/library/detail.aspx?g=f838e758-6ee2-4363-946b-323bcd13079b)

[6] The UIGEA prohibits gambling businesses from "knowingly accepting payments in connection with the participation of another person in a bet or wager that involves the use of the Internet and that is unlawful under any federal or state law." The act specifically excludes fantasy sports that meet certain requirements. (Source: https://www.lexology.com/library/detail.aspx?g=f838e758-6ee2-4363-946b-323bcd13079b)

[7] On Jan. 20, 2021, the U.S. Court of Appeals for the First Circuit issued a potentially historic ruling in New Hampshire Lottery Commission et al. v. Barr et al., by rejecting an appeal brought by the U.S. Department of Justice (DOJ). The DOJ's appeal created uncertainty for the future of the online gambling industry. Essentially, the Court reaffirmed a June 3, 2019 decision, issued by a federal district court judge in New Hampshire, finding that the Wire Act applies only to gambling activities on sporting events and does not prohibit other forms of gambling conducted over the internet—including online casino gaming (iGaming) or online lotteries (although iGaming or online lotteries may be prohibited by other laws in various states). (Source: https://www.lexology.com/library/detail.aspx?g=f838e758-6ee2-4363-946b-323bcd13079b)

[8] However this decision may also be impacted by other State laws.

[9] Interview with Gaming Executive

[10] James Banks and David Moxon, *"UIGEA and the rise and rise of gaming and gambling in the UK"* Crimetalk, January 2012 https://www.crimetalk.org.uk/index.php?option=com_content%5C&view=article%5C&id=622:uigea-gaming-and-gambling-uk%5C&catid=38:frontpage-articles%5C&Itemid=41

and the United Kingdom (UK).[11] A preliminary analysis of jurisdictions offering regulatory services for online gambling shows a wide range of regulatory standards - from tightly controlled to very little regulation at all. In well-regulated jurisdictions, the gambling oversight agency or another oversight body like the financial regulator ensure that the payment methods accepted online are regulated within the jurisdiction that they originate from as part of the overall gaming regulation, however, this rule does not hold true in all jurisdictions reviewed.

How do criminals launder money through land-based casinos?

To understand the money laundering vulnerabilities of online gambling operators, we first need to consider the AML risks linked to land-based casinos. Interviews with compliance staff from US land-based casinos still highlight vulnerabilities with third-party payments including the use of large cash-based transactions. Of significant concern is also smaller players structuring payouts along with bill stuffing. The onboarding process for clients/gamblers in a land-based casino is also not as comprehensive as a banks or financial institutions. For example: a casino client may only be subject to customer due diligence ("CDD") checks for amounts over $1,000. For high-rollers, enhanced due diligence may be triggered at $500,000 to understand the client and their source of wealth/funds according to industry experts. Marketing hosts can play a role in collecting preliminary due diligence data from a customer and this is then verified by the compliance department. The casino may seek to obtain an attestation from the client relating to the source of funds or other important due diligence information.

Casinos, both land-based and online, are often considered high-risk for AML/CFT with some banks prohibiting client accounts completely if they are linked to casinos. In some jurisdictions, land-based casinos open bank accounts and financial services relationships through holding companies without reference to any gambling activity to enable access to financial services due to the high-risk perception of the industry. This prohibition and restriction on banking services has led the industry to innovate other payment methods that patrons can easily access, and the casino can readily accept. Casinos fall under the Designated Non-Financial Businesses and Professions (DNFBP) sector under AML rules which, depending on the national legislation, are required to report suspicious transactions and activity (STR/SAR) to the nation's financial intelligence unit. The reasons that casinos have traditionally been considered high risk for money laundering include:

- The historical cash-intensive nature of the business.
- The range of financial services that are offered in casinos, often over extended hours (i.e.: foreign exchange, cheques, cash, wire transfers, etc).
- The historical linkages to organised crime as beneficial owners of casinos.
- The activities of junket operators and VIP rooms where the origin of funds is unclear (i.e.: this could be the proceeds of crime. Front money can also be extended by junkets for their VIP patrons and paid back).
- Loan sharking, proxy betting and employee complicity also pose significant risks.

There are numerous examples of the proceeds of drug crimes being laundered through land-based casinos. The British Columbia (BC) casinos in Canada have some of the most well documented examples where bags of cash were brought into the casinos to convert to casino chips, play a few games and cash out as clean money (sometimes known as short play). Unlicenced money businesses are also playing a key facilitation role. In the US and Canadian markets, cases of unlicenced money transfer businesses lending gambling patrons funds to

[11] Mr Gamble Website: https://mr-gamble.com/uk/

gamble has been more commonplace. The origin of the funds is often unknown and can be potentially from the proceeds of a crime (these have historically been linked to drug crimes). The funds from the unlicenced MSB are loaned to the gambler, and the gambler will repay the funds within China where only a domestic transaction will occur. This "scheme" also assists in circumventing China's currency controls and allows access to capital to gamble in different countries. It also allows the money operator to convert cash from the US, for example, into a bank deposit within another country like China.

Some of the most powerful junket operators from Hong Kong are now under pressure partially by being implicated in the Australian government inquiry into Crown Casinos putting focus on how junket operators may facilitate money laundering. Another significant event is the arrest of Alvin Chau in December 2021, CEO of the Suncity Group junket in Macau on illegal gambling charges. Sun City and other junkets (known as independent agents in the US) can often extend front money for the customer to gamble, however this leaves a large vulnerability around the source of the funds and that the funds are not criminal proceeds. Junkets can be listed companies on the Stock Exchange in Hong Kong which are generally perceived to be legitimate.

Underground Banking Case Study (UK)
The UK authorities assessed that some of the cash spent in casinos in the UK was linked to South East Asian underground banking networks. Due to capital flight controls, South East Asian nationals wishing to gamble in the UK utilise the services of underground bankers to make cash available for them in the UK which would not be possible using the regulated banking sector. The South East Asian national makes a bank transfer to the underground banker within their domestic jurisdiction. Once they arrive in the UK, they can then collect the equivalent amount of cash from the underground banker's contact. However, this cash is usually the proceeds of crime, which the contact has laundered on someone else's behalf.

(Source: United Kingdom National Risk Assessment 2020)

The implementation and deployment of the 'digital yuan'

Given the significance of the Chinese tourism market and the junket trips to land-based casinos we also briefly consider the launch of the digital yuan, a new Central Bank Digital Currency ("CBDC") in China. It is anticipated that the new digital currency may be trialled in Macau with the potential to "curb money laundering" linked to casinos and the junket industry.[12] The currency allows the Central Bank of China to track transactions which would reduce the potential for illicit transactions. A recent article speculates how China could deploy the new CBDC for casino and gambling purposes. "*It remains to be seen whether Macau might simply allow its casinos the option of adding the digital yuan to their list of funding options or whether the digital currency would become the only permissible option. The latter could have a significant impact on local junket operators, with a knock-on negative for the casinos themselves."*[13] Those that gamble in Macau may be reluctant to use the digital yuan because it exposes their identity to the Chinese government, and if this becomes the only permissible option, the players may move to other gambling destinations.

[12] Farah Master, "*Macau's digital yuan plans to deal fresh blow to casino junkets",* Reuters, April 2021 https://www.reuters.com/world/china/macaus-digital-yuan-plans-deal-fresh-blow-casino-junkets-2021-04-22/
[13] Steven Stradbrooke, "*Macau steps closer to digital yuan use in casinos*", Coingeek, April 2021 https://coingeek.com/macau-steps-closer-to-digital-yuan-use-in-casinos/

Cashless gaming for land-based casinos

Technological advancement in online payments platforms have also been re-shaping the way land-based casinos operate. Land-based casinos and integrated resorts are now introducing *"cashless gaming systems"* where casino patrons can use QR codes to conduct their gaming activities at the slot machines. Cashless gaming works by downloading an app, walking up to the slot machine and showing your QR code which is generally tied to a bank account and /or rewards program. The app will verify the identity of the player and link to digital payment providers (i.e.: Paypal, Applepay) including banks to provide a new cashless alternative to gaming. Technically, the funds paid from the bank account or through the digital payment providers could still contain criminal proceeds, however cashless gaming apps may place some of the due diligence burden on the payment provider. Theoretically, these payments will make the source of funds more traceable. The American Gaming Association suggests that: *"the widespread adoption of digital payments in gaming will offer compliance teams and regulators better oversight and improve know your customer (KYC) and anti-money laundering (AML) capabilities.*[14] However, in the US market, the Bank Secrecy Act ("BSA") rules do not allow a regulated entity (casino) to rely on another entity for its BSA obligations. The casino is still required to have robust processes and procedures in place to ensure adequate AML safeguards are in place to use cashless gaming systems.

For further granular examples of AML vulnerabilities in land-based casinos, refer to the FATF Guidance papers.

1. FATF Guidance on the RBA for Casinos (2008)
2. Vulnerabilities of Casinos and Gaming Sector (2009)

[14]The American Gaming Association, "*Payment Modernization",* 2022 https://www.americangaming.org/policies/payment-modernization/

Section 2: Online payments & the associated AML vulnerabilities

The proliferation of alternative online payment methods

Traditional payment methods can include bank transfers, credit cards, cheques, and money remittances. **Alternative payment systems** are newer innovative payment methods such as e-wallets, pre-paid cards, online third-party payment providers (i.e.: Paypal), and cryptocurrencies.

The number of alternative payment providers has increased due to increased demand for online payment systems including the adoption of local and regional mobile money systems, online payments like Paypal and Stripe, online prepaid cards along with e-wallets and crypto wallets. Third party payment providers have evolved from the early 2000s alongside the development of the internet to facilitate online and electronic commerce transactions. These payment providers are often classified as Money Service Bureaus (MSBs) for regulatory purposes. Guidance issued by the US financial regulator FinCEN in 2012 and 2014 defines payment processors that are required to register with FinCEN as MSBs and are subject to the BSA. In this context, some payment processors fall outside FinCEN's definition including those referring to themselves as "technology companies" and are, therefore, not required to register as MSBs or subject to the BSA and hence are not subject to regulatory oversight."[15][16] The test within US markets is whether third party payment providers are moving money or facilitating it. The third-party payment providers argue the latter, that they are not moving money, merely facilitating it.

Traditionally, both land-based and online casinos have been subject to a number of banking restrictions and scrutiny which has encouraged the adoption of alternative payment systems. The types of payment methods available for online casinos are often dictated by the target market of the casino and the jurisdictions it operates within. With casinos that are available in multiple jurisdictions, payment methods can often be tailored to the location of the clientele with regional payment methods being widely offered. These regional payment methods also assist in restricting traffic from other locations where gamblers may access casino services with the use of a Virtual Private Network (VPN). For example, if there was a casino offering services in Kenya, M-PESA may be available but if the casino operates from Russia, regional payment platforms would be available making it difficult for a Kenyan to play at this casino.

As part of this research, several online casinos were visited and sampled at random to identify key data on how payments are facilitated. The key payment methods are classified into six main groups, noting that payment providers can often fit into more than one payment method as illustrated below:

[15] FINCEN Advisory and Ruling 2012 and 2014 https://www.fincen.gov/sites/default/files/administrative_ruling/FIN-2014-R009.pdf https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2012-a010,
[16] Interview with Gaming Executive, 2021

Payment Methods	Payment brand examples
1. Traditional Banking	Debit, Credit, Visa, Mastercard, Wire Transfer, ACH
2. E-Wallets	Skrill, NETeller, ecoPayz, CashU
3. Prepaid Cards	Neosurf, FlexEpin, Paysafecard, Ecovoucher
4. Cryptocurrency	Bitcoin, Ethereum, Bitcoin cash, Litecoin
5. Mobile Banking	WeChat, Moneta.ru
6. Online payments & third-party payments	Paypal, Applepay, Square, Stripe, etc.

E-wallet providers Skrill and NETeller owned by Paysafe are extremely popular in the online gambling markets, both are regulated in the UK by the Financial Conduct Authority (FCA). Skrill and NETeller provide a range of deposit and withdrawal options including cryptocurrency, credit and prepaid cards, and require some basic ID and proof of address documentation as part of the sign-up process.

Paysafe, the owner of Skrill and NETeller was recently accused of processing transactions linked to Italian mafia groups. An article published in October 2020 reports how the payment providers Skrill and Neteller may have been used to process hundreds of thousands every week between 2011 and 2018 which highlight AML vulnerabilities in the e-wallet providers payments infrastructure. Until 2017, the online gambling platform *Centurionbet's Bet1128* was suspected of ties to Italian mafia groups before its licence was suspended by the Maltese gaming authority. The Investigative Reporting Project in Italy reported that the beneficial owner of the casino made the online operation available to mafia groups for money laundering purposes.[17]

The recent demise of Wirecard has also raised some questions about the "close associations" of the payment providers with online casino operators. Wirecard was a payment processor headquartered in Germany that was shut down in 2020 after $1.9b went missing linked to the Philippines subsidiary. Wirecard built its business in the early 2000s catering to the gambling market but there were allegations in the "*Zatarra Report"* [18] that Wirecard owned a number of online casinos and adult websites and miscoded transactions to circumvent government controls. Miscoding transactions has been relatively commonplace in the online gambling markets historically to avoid government scrutiny. A charge may appear on your credit card as "*flowers"* for example making it difficult to identify gambling transactions. Third party payment providers have had some run-ins with US law enforcement linked to facilitating online gambling and the associated money flows from US citizens. Whilst an older case, the NETteller case demonstrates the long arm of US law enforcement and how payment processing companies can be implicated in transactions where online gambling may be deemed illegal. The premise of the case was that NETeller was processing transactions from the US where gambling was illegal and facilitating illegal gambling by US individuals.

[17] Matteo Civilini, *"E-money giant Paysafe processed mafia-linked transactions*", Investigative Reporting Project Italy, October 2020, https://irpimedia.irpi.eu/en-paysafe-e-wallets-mafia-transactions/
[18] Viceroy Research, "*Zatarra Research and Investigations -Wirecard",* Viceroy Research, July 2020 https://viceroyresearch.org/2020/07/03/zatarra-research-investigations-wirecard-reports/

NETELLER Case Study

NETeller was founded by two Canadians, Lawrence and Lefebvre, and went public in the UK after relocating from Canada to the Isle of Man in 2004. In 2007, the DOJ charged both founders with laundering billions of dollars in internet gambling proceeds. The two were arrested for: the creation and operation of an internet payment services company that facilitated the transfer of billions of dollars of illegal gambling proceeds from United States citizens to the owners of various internet gambling companies located overseas.

The press release stated that NETeller provided 80% of worldwide gaming merchants with payment processing services. These services allowed the collection of US-based funds to be transferred to bank accounts outside of the US. The founders pleaded guilty, while NETeller admitted wrongdoing and reached a $136 million settlement with U.S. authorities. After losing out on its largest market in America, NETeller shifted its focus to Europe. "*The case of NETeller demonstrates how gambling operators can utilise third party operators as conduits through which to hide the true nature and purpose of financial transactions whilst engaging in money laundering*."

Source: Department of Justice Press Release, January 2007
https://www.justice.gov/archive/usao/nys/pressreleases/January07/netellerarrestspr.pdf

How can criminals launder money through online casinos?

Moneyval is[19]the FATF-style body for Europe which monitors AML/CFT trends and standards across Europe. Moneyval issued a report in 2013 on the use of online gambling for money laundering and financing of terrorism purposes that suggested that there are three types of jurisdictions that can be identified linked to online gambling. These have been further classified in this paper as white, grey, and black markets.

1. White Markets	Jurisdictions where online gambling is both legal and regulated.
2. Grey Markets	Jurisdictions where online gambling is legal but not regulated. This may pose vulnerabilities without proper regulation.
3. Black Markets	Jurisdictions where online gambling is illegal. Where gambling is illegal, there may be some business practices like miscoding the credit card clearing codes to ensure the activity remains undetected.

Both grey and black markets pose the greatest vulnerabilities for money laundering linked to online casinos due to the lack of regulatory oversight and the potential deceptive measures that may be undertaken by black market operators to avoid detection. Moneyval reports that in legal (white) online markets, money laundering was cited as less common due to:

1. Gamblers being subject to customer identification controls and therefore their identity would be known.

[19] Moneyval is the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing ofTerrorism. Moneyval assesses compliance with the international standards to counter money laundering and the financing of terrorism and the effectiveness of their implementation, as well as making recommendations to national authorities in respect of necessary improvements to their systems.

2. Financial transactions related to online gambling are conducted electronically and are therefore easily traceable and
3. All wagering carried out by online gambling operators is recorded.

In grey and black markets however, customer identification is still vulnerable with multiple reports linked to stolen identity data used as identification. There are also anonymous payment methods that can be used in a selection of online casinos if criminals should wish to launder via the casino, or they could perhaps even own or control one. Ingo Fiedler[20] defined eight factors that make online gambling susceptible to money laundering in a 2013 article. "*The virtuality of products and cash flows, the international nature of the cash flows, the complexities associated with payment processing, the legal and illegal nature of the gambling markets, the non-harmonization of laws, and grey areas within existing law along with the high payout percentages, and tax-free winnings in some jurisdictions."*.

Based upon a review of multiple jurisdictions and case studies, the most significant AML vulnerabilities identified specific to online casino operators include non-face-to-face transactions, the potential for third party transactions, the difficulty in verifying source of funds, the beneficial ownership of the casino and/or payment provider, and inadequate CDD policy implementation by the casino operator. These are explained in detail below:

1. **Non-face-to-face transactions (Anonymity)** Non-face-to-face business relationships can present unique AML risks around identification and verification of the customer registering for the online gambling account. Case studies highlight that stolen identities have been frequently used for online gambling purposes. Another vulnerability includes a player profile being set up with a stolen ID or given to a third party to access the account for the facilitation of transactions of high-risk clients, i.e.: clients that may be criminals, high-risk (PEP[21]), or subject to sanctions without the appropriate enhanced due diligence procedures. Controls should be put in place to mitigate this risk to ensure adequate screening is conducted on each player. This could be live or photographic evidence of the person with the appropriate government-issued ID for example to ensure it's the same person. Verification of identity procedures should also be implemented that include a periodic review of the client information and identity.

2. **Third Party Transactions** – Technically a vulnerability linked to the non-face to face nature of online casinos, third party transactions are one the biggest vulnerabilities of online casinos where money deposited by one player could be withdrawn and deposited into another party's account. If Player A deposits via an e-wallet, he/she can then potentially withdraw to a crypto address that is owned by another party – this transaction could take place as payment for drugs, for example. If the casino is registered in a well-controlled jurisdiction, it is likely this can be mitigated with controls on depositing and withdrawing funds through the same payment method. In the above example, linked to non-face-to-face transactions, the accounts can also be infiltrated or sold to other parties creating additional risks for the casino operator.

3. **Source of Funds Verification:** The source of funds verification often relies in some way upon the payment providers due diligence processes. If an online player uses bank deposits,

[20] Ingo Fielder, "Online Gambling as a Game Changer to Money Laundering, SSRN Electronic Journal, April 2013,https://www.researchgate.net/publication/254969899_Online_Gambling_as_a_Game_Changer_to_Money_Laundering
[21] PEP is a Politically Exposed Persons. These are generally high-level government officials that are classified as higher risk for money laundering purposes.

the online casino may rely upon the bank's due diligence procedures linked to the source of funds, however, the online casino is still responsible for reporting suspicious transactions which could include multiple deposits from prepaid cards, for example. Additional AML/CFT vulnerabilities include the use of alternative payment methods that are not regulated, financial intermediaries that are not subject to adequate AML/CFT controls, and the use of anonymous prepaid cards which breaks the chain of identifying the original source of the funds. Monetary transfers between online player accounts (peer-to-peer) should also be discouraged as it creates opportunities for in-game funds transfers that could be used for illicit purposes. These types of transfers may be seen for card games like poker, for example. Cryptocurrency and stored value cards pose the most significant AML risks due to the difficulty in verifying the real origin of funds when depositing for game play. Some casinos will accept bank deposits with the ability to cash out in cryptocurrency to avoid the "burden" of verifying the source of funds. i.e.: they will not take crypto deposits, but they will allow crypto withdrawals.

4. **Beneficial Ownership:** The risks associated with criminal elements owning or infiltrating an online casino was deemed high by many jurisdictions reviewed. The ownership by criminal elements of a payment provider provides an even higher risk for potential money laundering. The risks around criminal elements owning, controlling and/or infiltrating the casino along with criminal elements owning and/or controlling the payment provider should be actively managed and monitored.

Case Study 1: Beneficial Ownership of Casinos

An eCasino notified the Alderney Gaming Control Commission ("AGCC") that it has been taken over by a new beneficial owner. The AGCC investigated the fitness and propriety of that beneficial owner, and during the investigation, information was obtained that led the AGCC to be suspicious of the source of funds of the beneficial owner. As a result, a SAR was made by the AGCC to the FIU. This led to a multi-agency operation involving other jurisdictions, resulting in the beneficial owner being arrested in a foreign jurisdiction on suspicion of tax fraud and money laundering. The licence was immediately suspended and a date was set for a revocation hearing. No hearing was necessary as the licence was surrendered.

Source: Bailiwick of Guernsey National Risk Assessment

5. **Inadequate AML/CDD policy implementation** – Selected jurisdictions reported that there were concerns around the implementation of AML due diligence policies and procedures by online operators. The lack of understanding and lack of prioritisation of risk management, internal controls and anti-money laundering was highlighted and recommended to be regularly assessed. Gambling oversight agencies often resolve any breaches of AML through administrative sanctions and other enforcement tools depending on the jurisdiction. We consider some recent enforcement cases and administrative sanctions in **Section 3**.

AML risks linked to online casinos and virtual currencies

Bitcoin is often referred to as transparent payment method as the blockchain cannot be altered. However, linking a Bitcoin address to a real-world person can be challenging. Blockchain investigation tools can assist in identifying if the Bitcoin address has been linked to fraud or other suspicious activity but the linkage to a real-world identity often relies upon the fact that the cryptocurrency has been traded on a compliant exchange that is required to obtain AML/CDD documentation from the client when buying and selling the Bitcoin. This is referred to as pseudo-anonymity. Altcoins are also accepted for many online casinos and are becoming more popular as a payment mechanism that is globally acceptable that has low associated transaction costs. If cryptocurrencies are purchased through peer-to-peer networks, the source of funds can become even more obscure, and the money laundering risks heighten.

While many jurisdictions have not yet permitted the use of cryptocurrencies for online gambling due to the fact that cryptocurrency is not yet regulated by the national financial regulator, the Isle of Man has adopted the use of cryptocurrencies for gambling online. The Isle of Man (IOM) Gambling Supervision Commission (GSC) has issued comprehensive guidance on the AML/CFT risks associated with virtual currencies. The IOM has made changes to existing regulations to allow operators to accept deposits in money or "money's worth". This includes CVCs and VCs explained below:

1. **CVCs** – Convertible virtual currencies. CVCs include cryptocurrency that can be bought and sold through various exchanges.

2. **VCs** – Non-convertible virtual currencies. VCs include digital "skins" for avatars or items such as weapons within video games. VCs also include currencies that exist within the context of a specific game for the purpose of buying in-game items, etc. VCs differ from CVCs in that they are not used in the same way as fiat currency and are not broadly used as a method of payment.

The guidance issued includes reference to electronic gaming items which often fall under the purview of the gaming regulator although a newer emerging area for regulators. There are many identified risks associated with allowing crypto gambling. These include: the lack of expertise by governments in dealing with new and developing technologies, the difficulty in linking the account to a real-world identity, the potential use of anonymity software – coin and IP mixers, difficulties in establishing the source of funds and source of wealth, and the lack of AML/CFT controls for CVC/VC in many jurisdictions.[22] The Isle of Man provides guidance to mitigate these risks including matching the IP and address details, conducting enhanced due diligence on transactions that link to anonymiser software, IP mixers, coin mixers and anonymity enhanced crypto-currencies, conducting online adverse media checks and using block chain analysis tools to check if a wallet has been exposed to any fraudulent or suspicious activity. The advice given also suggests setting lower thresholds for crypto gamblers, in the Isle of Man this limit is set at EUR3,000.

[22] Gambling Supervision Committee, "*AML/CFT Guidance for Virtual Currencies 2020"* Isle of Man, 2020 https://www.gov.im/media/1371388/vc-aml-guidance-2020.pdf

Prepaid (stored value) cards

Prepay cards also known as *"stored value"* cards demonstrate a unique ability to break the chain of the source of funds and can facilitate a complex layering of criminal proceeds. The client can purchase prepay cards and use them online to gamble. There are multiple types of prepay card:

1. Reloadable prepaid cards	Often issued and linked to a bank account and can be issued by Visa or Mastercard for example.
2. Disposable prepaid cards	Cards issued are often used only once and not reloadable.
3. Virtual prepay cards	Virtual cards operate in a similar manner as plastic cards but are issued virtually to be used online – i.e.: the codes and numbers are sent online. Often linked to Visa but in some cases can be loaded with cash. Issued by Skrill (online vouchers issued). Neopay is also an online voucher system that can be used to pay for goods online.
4. Crypto prepay cards	Crypto prepay cards are debit cards that can used to pay for everyday goods loaded with various cryptocurrencies that are used to pay for goods in fiat currency.

Prepay cards are often an available option to fund betting accounts but the money often needs to be withdrawn through another payment method like a bank account or cryptocurrency first. Anonymous prepay cards including Neopay are also available on some sites.

Key vulnerabilities of prepaid cards in the context of online casinos:

- Can be anonymous and has the ability to obscure the source of funds.
- Usually only used as a deposit method which requires a different withdrawal method.
- Can be used as a money laundering mechanism as part of the "layering" of funds stage.
- Can also be used to pay third parties as part of criminal transactions.

Casino simulation (walk-through)

Two online casinos were selected at random to conduct a walk-though to further understand the operations of the casino and the associated AML requirements.

Casino #1 was registered in a UK offshore jurisdiction and available from Canada. The casino operated in a number of countries with a selection of payment methods. A casino, live casino, sports book, and virtual sports option was available with over 1200 slot games of varying themes. The following payment methods and AML controls were documented:

Payment options	Visa, Mastercard, Skrill 1-tap, Bank transfer, Paysafecard, Visa Debit, Visa Electron and Maestro. Note that e-wallets like Skrill are often funded by various means including from bank accounts or with cryptocurrency before being used for a gambling transaction therefore a gambler may fund his/her Skrill account with crypto to gamble in an indirect manner.

Required AML documentation	A valid Government-Issued ID was required for accounts at Skrill or NETeller before funding the accounts used to gamble online along with a paper-copy confirmation of address (i.e.: a utility bill) before the account was activated. If these payment platforms are not used (Skrill or NETeller), the casino will request key forms of identification, usually limited to a proof of ID and a proof of address which will be verified before play is allowed.

The casino also provides guidance around using pre-paid cards where anonymity is important or when you don't want to deposit more money than you can afford. Citadel Instant Banking (*My Citadel)* was also an option offered to transfer money to the casino account anonymously. Paypal, mobile deposits (Boku), Sofort (a German payment provider) and MuchBetter, a smartphone app that allows payments from e-wallets and traditional banking sources were also payment options along with mobile payments that can be made via a UK phone bill. While the website details a number of payment methods including the use of Neopay prepaid cards (vouchers), to actually use these cards was not possible from Canada, which was the jurisdiction the betting was taking place from. It also states that Paysafecard can be purchased with cash, "leaving no trace of who you are" demonstrating that anonymity of payments is permissible in this selected regulated operator.

The second casino, **Casino #2** was registered in the Caribbean islands and available from Canada) with a .eu extension website. This casino offered a sports book, casino operations, live dealers, poker, and horse betting. The casino was much more limited in the payment methods accepted and relatively difficult to use for those not already involved in purchasing and using cryptocurrencies. It could be considered close to a real "crypto-casino," however, it did also offer some traditional payment methods including Visa, Mastercard, and Interac e-transfer.

Payment options	Bitcoin – BTC, BSV, Litecoin, Ethereum, BitcoinCash, Visa, Mastercard, and Interac-e-Transfer
Required AML documentation	Bank and credit card deposits were subject to checks with government-issued ID. The terms and conditions did refer to some AML policies including the prohibition of multiple accounts and the transfer of funds between player accounts. Cryptocurrency was not yet regulated by the government within the jurisdiction where the casino was regulated and registered.

Section 3: Regulatory and enforcement considerations

Since the introduction of online gambling services in the 1990s, the industry has grown with a number of globally recognised regulators with specific expertise in regulating online gambling activities. Licencing online gambling can be a lucrative activity for governments if they can ensure robust guidelines for the online operations and mitigate any risks associated with attracting criminal activity. According to Mr-Gamble.com (Mr. Gamble), a website that assists in finding online casinos by jurisdiction, deposit type, language and game provider, there are 14 key jurisdictions listed to choose from with respect to the online casino market. These include: The Isle of Man, Malta, Gibraltar, Curacao, Alderney (Guernsey), Kahnawake (Canada), Costa Rica, New Jersey (USA), Denmark, Italy, Estonia, Spain, Sweden and the United Kingdom (UK).[23]

Mr. Gamble also allows a user to sort online casinos by the payment type. There were 103 payment methods listed on the Mr. Gamble website which included: cryptocurrencies, banks, mobile money transfers, prepaid and stored value cards, along with digital payments and e-wallet services. The research observed two key themes as part of the casino walk-through simulations:

1. **Online gambling is often restricted to selected jurisdictions:** Online casinos are often available in selected and approved jurisdictions, although by using a VPN[24] a user is able to easily locate casinos that are not normally available in their country of residence. In many cases, online casinos are regulated in one jurisdiction and available to players in secondary markets (i.e.: not available in the country of registration). For example, a casino registered in Antigua may serve markets in Canada and is not accessible to local Antiguans.

2. **Payment methods depend on the target market:** Payment methods for online casinos are tailored to the clientele in the target market. i.e.: Russian payment systems are used when the online casino is available to Russian clientele and Chinese payment systems are available for Chinese clientele for example. WeChatPay and Alipay are both popular payment platforms in China and are available for some gambling sites listed, however, gambling is illegal in China therefore it is likely subject to enforcement action by government officials in-country. For online casinos operating in multiple jurisdictions, payment methods can differ based on the location of the client/gambler.

The online market has matured significantly over the last ten years. While regulation was originally conducted at the Point of Establishment ("POE"), it has now moved to the Point of Consumption ("POC"). The POE is where the casino is registered and generally where the servers are based whereas the POC is where the players are gambling from. For example: an online casino in Alderney may target players in the UK market. Regulations have shifted to ensure the consumer is appropriately protected and this has required gambling operators to register in the jurisdictions it is serving i.e.: the UK. A recent fine by the UK Gambling Commission fined an Alderney company highlights how this has been changing and the STR is filed in multiple jurisdictions, in this case Alderney and the UK. Online operators are largely dependent on the target market jurisdictions and also rely upon the payment methods that can be offered within those jurisdictions.

[23] Mr Gamble Website https://mr-gamble.com/uk/
[24] VPN – Virtual Private Network

Illegal gambling and blacklists

The proliferation of unlicensed online gambling operators has been highlighted as a concern amongst gaming regulators. When operators are unlicensed, compliance with existing laws, the integrity of game offerings, and security of players are sacrificed. It also deprives the government of licencing revenues. Illegal gambling operators trade without a licence and without regulatory oversight. When illegal operators are detected, they are often referred to national police units and, in some cases, listed on the gaming authority websites under "Blacklists." Regulators suggest that it is not always easy to take action against illegal operators as they often operate outside of the jurisdiction. Enforcement registers and blacklists are kept by many countries including Malta, for example, which maintains an enforcement register showing the cancellation and suspension of gaming operators.[25]

A recent article published by Dutch journalists, "Follow the Money," suggests that around 12,000 sports betting and casino gaming websites operate on the island of Curacao which are said to make up nearly 40 percent of the global unregulated supply.[26] The article further states that online casinos registered in Curacao have appeared multiple times on blacklists maintained by various regulators. Curacao has recently come under pressure from the Dutch Government for its role in blacklisted gaming activity and has been told to reform the industry. The 2021 investigation found that 40% of all blacklisted companies in 18 countries have been traced to one address on the island as part of the investigation. According to Vixio, a gaming compliance and research platform, being placed on such a list usually means that governments or regulators require internet providers, and in some cases also payment processors, to block the domain names of unlicensed casinos. The Curaçao government does not actively pursue the unregulated gambling sector providing vulnerability to players using Curacao-registered websites. Not all countries have a public blacklist, for example the Netherlands does not. But Poland, Turkey, Russia, Belgium, Sweden, Australia, and Greece, among others, do.[27]

The Isle of Man Gambling Supervision Committee (GSC) also recently published a notice on their website suggesting that black-market operators are claiming to be regulated by the GSC. They state that, *"We have become aware of a number of gambling websites, which claim to be licensed by us, but which are not. When we become aware of these sites, we list them on our website's rogue's gallery."*[28]

With multiple restrictions on gambling activity in South-East Asia, including its illegal status in China and Thailand, authorities have also been leading efforts to combat illegal online operators. The Thai authorities recently arrested several suspects linked to online casino Royal Slot 777, an app available since 2019. The investigation led back to a Chinese national that had 10 different companies registered that are suspected of being money laundering fronts.[29] Another recent case in Vietnam also charged public officials with illegally running an online betting website.

[25] Malta Gaming Authority, MGA Enforcement Register: https://www.mga.org.mt/mga-enforcement-register/
[26] Henk Willem Smiths and Remy Koens, "Follow the money: Curacao is a paradise for illegal online casinos", Follow the Money, November 2021 https://www.ftm.nl/artikelen/casinos-op-curacao
[27] Henk Willem Smiths and Remy Koens, "Follow the money: Curacao is a paradise for illegal online casinos", Follow the Money, November 2021 https://www.ftm.nl/artikelen/casinos-op-curacao
[28] Gambling Supervision Commission, Isle of Man. https://www.gov.im/about-the-government/statutory-boards/gambling-supervision-commission/
[29] Onlinecasinos.com "*Thai Police arrest suspects in online gambling crackdown*" https://www.online-casinos.com/news/society/thai-police-arrest-19-suspects-in-an-online-gambling-app-crackdown.html

The role of the regulator and other government agencies

1. The gaming regulator and/or gaming oversight agency

Often referred to as the gaming oversight authority, the gaming regulator is responsible for licensing online gambling operators and for ensuring gaming operators have the appropriate internal controls and AML procedures in place. The scope of regulation can range from card games to electronic gaming. All forms of gambling organisations are licensed or certified from *integrated operations* which have direct customer relationships and manage their own betting platforms to those who seek to operate the platform developed by a another provider. In addition suppliers of games and services can also obtain certification. While not all countries have a dedicated gaming regulator, most prominent jurisdictions do. Costa Rica is the most obvious exception to the rule that does not maintain a dedicated gaming regulator but does maintain a significant presence in the registration of online casinos. Online casino operators do not pay for a licence as it is managed as an ordinary company. Costa Rica is also known to be crypto friendly so it attracts online operators that want to use cryptocurrency to facilitate payments.[30] In the US, regulation of gambling is decentralized and is not regulated by the federal government. Gambling is licenced at the State-level and through tribes in the United States. Online gambling is legal in at least seven US states currently: Connecticut, Delaware, Michigan, New Jersey, Pennsylvania, West Virginia,[31] as well as Nevada which allows online Poker. Online sports betting is legal in 29 states.

Enforcement and regulatory strategies

Legislative fines and penalties coupled with administrative sanctions are often available for application by gaming authorities when an operator is in non-compliance. Fines for both social responsibility breaches (allowing problem gamblers to gamble) and for anti-money laundering failures are common. Other tools in the enforcement toolkit include administrative sanctions: revoking or suspending the gaming license, cautioning the casino and requiring remedial actions to be undertaken, for example. Comprehensive risk assessments, internal control frameworks, and regular reporting on trends (i.e.: stolen licences, STRs, etc.) are required by operators to stay in compliance and to mitigate potential risks.

The Gibraltar Gambling Commissioner conducted a risk assessment of the gambling industry as part of the National AML Risk Assessment process to highlight potential risks. This risk assessment identifies five key areas and provides a useful framework to categorise key risks associated with online gambling.

Risk Areas	Potential Types of Risk
a) Internal Control Vulnerabilities	This can include situations where an online operator does not adhere to their own policies – i.e.: failure to implement AML compliance policies, adherence, and to apply periodic review procedures to comply with regulatory standards etc.
b) Licensing and Integrity Vulnerabilities	Where criminals act as casino operators or staff or have infiltrated the casino to exert some control.

[30] Fast Offshore Website, Costa Rica Gaming Licence, Does it exist? https://fastoffshore.com/what-we-do/packaged-services/costa-rica-gaming-license/

[31] BettingUSA.com https://www.bettingusa.com/states/#:~:text=How%20many%20states%20have%20legal,%2C%20Pennsylvania%2C%20and%20West%20Virginia.

c) Customer Related Vulnerabilities	Customers that are able to sign up that may be PEPs or sanctioned individuals for example.
d) Product Related Vulnerabilities	The types of games that are played. i.e.: poker and peer-to-peer gambling provide a higher risk or vulnerability of money laundering.
e) Payment Method Vulnerabilities	i.e.: E-wallets and prepaid cards[32]and the associated fraud and money laundering risks.

Government oversight mechanisms for online gambling

Regulation of the payment providers is often the mandate of a different government agency and usually falls within the mandate of the financial regulator. The role of the gambling authority is often to mandate that only regulated payments should be offered – even if those payments are regulated by a separate authority in-country or internationally. For example, if an Alderney-registered casino operator wishes to use e-wallet services from Skill and NETeller, it is permissible as these payment providers are regulated by the UK Financial Services Agency (FSA). If an online casino wants to use cryptocurrency and is based in Alderney, it cannot as the Guernsey Financial regulator has not yet endorsed/regulated payments with cryptocurrencies. The financial regulator can play a key role in the regulation of payments linked to online casinos and work closely with the gaming authority on the payments landscape. The financial intelligence unit also plays a key role in receiving suspicious transaction reports (STRs) and, in some cases, shares these reports with the gaming oversight agency to further inform the key risk areas. For example, in 2016, Antigua's Financial Intelligence unit, the Organization of Drug and Money Laundering Control Policy (ONDCP) published its most recent annual report showing that land-based casinos, internet gambling and sports betting companies were required to do remedial work to implement their AML-CFT obligations.[33] Reports show the online gambling sector reported 24 Suspicious Transaction Reports (STRs) in 2015 and 11 in 2016. Most of the suspicious activity reported was classified as fraud and unauthorised use of credit cards. The ONDCP also noted that it receives reports on any pay-outs over $25,000 as part of control mechanisms to combat money laundering. Analysis of STRs assists in understanding the risks and vulnerabilities within the online marketplaces and allows for corrective actions to be taken.

The final component of the government oversight infrastructure includes additional law enforcement functions. In many jurisdictions, the national police will be responsible for receiving complaints about illegal gambling operators. The tax authority may also be involved in investigating wrongdoing linked to tax offences and the non-payment of taxes due.

Recent enforcement actions by gaming regulators

Globally, enforcement actions are becoming more common as regulators apply their powers to non-compliant online operators. A sample of the more recent enforcement actions are detailed below and include reference to fines for AML failures and fines for social responsibility failings (failing to prohibit known problem gamblers, for example).

[32] Assessment of the Money Laundering and Terrorist Financing. Risks within the Gambling Industry in Gibraltar, 2021 https://www.gibraltar.gov.gi/uploads/Gambling/Documents/Risk%20Assessment%20of%20the%20Gambling%20Industry%20in%20Gibraltar%20-%202021%20Update.pdf

[33] ONDCP Annual Report 2016

Date and Location	Breaches/Fines
2017 (UK) Social Responsibility Breaches **- Fine.**	The UK Gambling Commission fined 888 Holdings £7.8m for failure to comply with the UK on problem gamblers by allowing them to gamble after they had selected to self-exclude from the sites.
2018 (Denmark) AML Failures **- Warning.**	The Danish gaming regulator **Spillemyndigheden** warned 888 Holdings as they failed to report suspicious activity and identify the source of funds of a client gambling large amounts in a short period of time. It was reported that: *"While 888 conducted a background check on the customer, the gaming firm allowed the customer to continue playing on their site for one month, even though the customer was unable to provide documentation for their income source. Even though no source of income was provided, 888 allowed the customer to play for another 30 days before taking the decision to close the account."*
2018 (UK) AML Failures **– Fine.**	William Hill was fined £6.2m for failure to prevent money laundering.[34]10 customers were able to deposit money linked to criminal offences, which resulted in financial gains for the group of around £1.2m.
2021 (Malta) – Tackling illegal operators.	**The Malta Gaming Authority** issued €2.43 million in financial penalties between January and June last year, as part of an effort to ramp up enforcement in the sector and tackle unlicensed gaming operators. The gaming regulator issued 11 warnings, 20 notices of breach and sanctions and nine administrative fines. It also suspended two licenses and cancelled seven.[35]
2022 (Malta) Anti-Money Laundering Control Failures - **Fine.**	Online Amusement Solution Limited was fined with an administrative penalty of 386,567 by the **Financial Intelligence Analysis Unit** for anti-money laundering failures based on a site inspection of AML controls, policies and procedures. (Further details of the failings are provided in the administrative notice) [36]
2022 (UK) Gambling Commission **– Fine.**	Annexio (Jersey) Limited trading as Affiliate Empire was fined £612,000 for both Social Responsibility code contraventions, and breaches of the license condition put in place to combat money laundering and terrorist financing.

[34] Angela Monaghan, "*William Hill fined £6.2m by Gambling Commission*", The Guardian, February 2018 https://www.theguardian.com/business/2018/feb/20/william-hill-fined-62m-by-gambling-commission#:~:text=Betting%20group%20William%20Hill%20has,consumers%20and%20prevent%20money%20laundering.&text=It%20is%20the%20commission's%20second,failing%20to%20protect%20vulnerable%20customers.

[35] Jessica Arena, *"Gaming Authority issues €2.43 million in fines in the first half of 2020",* Times of Malta, February 2021 https://timesofmalta.com/articles/view/gaming-authority-issues-234-million-in-fines-in-the-first-half-of-last.851114

[36] FIAU Malta, Administrative Measure Publication Notice, January 2022 https://fiaumalta.org/wp-content/uploads/2022/01/Publication-Notice-20220114.pdf

Emerging trends - social gaming & crypto casinos

There were three key emerging trends that were highlighted as part of the research including the rise of illegal online gaming operators covered earlier. These include social gaming, the introduction of crypto casinos and blockchain gaming.

1. Social media gaming

"Social gaming" is defined as an online game played through social networks or social media. One jurisdiction surveyed reported that social media games connected to online casino sites were gaining traction. Social casino games were introduced as "gambling-themed games" that are online and accessed through social media sites or mobile apps. They are free to play and do not provide real money prizes, but you can use real money to purchase additional virtual (in-game) currency.[37]

Microtransactions are often used "in-play" to purchase virtual goods and have been relatively controversial in the gaming community with some countries banning the use of micro-transactions in games due to the gambling and addictive nature of how the games and transactions have been set up. The Netherlands has deemed that the purchase of lootboxes with microtransactions (tools in-game that can give you an advantage to win) constitute gambling and are therefore illegal.[38] Literature also suggests that these games are targeted at primarily young children. Traditional games like Fortnite and Roblox allow microtransactions and are also said to facilitate gambling behaviours.[39] There are some crypto exchanges that will exchange crypto-currency for in-game currencies, in-game currencies are also often traded in the real world for fiat currency and/or on black markets.

The Isle of Man has also observed a surge in "DIY-gambling" since COVID-19 and the use of social media and tele-conferencing apps such as Facebook, Zoom and Skype. The regulator has issued the following warning on their website as a COVID-19 update on 5 May 2020 "*If you use your computer in the Isle of Man to organise these without first having a licence, then you're breaking the law*." The Isle of Man has also issued AML guidance linked to in-game tokens that can be used as value-based exchanges.[40]

2. The rise of cryptocurrency payments and "crypto casinos"

Crypto casinos are also becoming more common and can be pure casinos (crypto only) or hybrid models where both traditional payments and cryptocurrencies exist. The acceptance of cryptocurrency is often dependent on the jurisdiction of regulatory oversight. In the Isle of Man, the Online Gambling (Amendments) Regulations 2016 allows operators to accept deposits in money or money's worth includes CVCs (convertible virtual currencies) and VCs (non-convertible virtual currencies). CVCs include cryptocurrency that can be bought and sold through various exchanges. VCs include digital "skins" for avatars or items such as weapons within video games and includes currencies that exist within the context of a specific game for the purpose of buying in-game item. The AML risks associated with cryptocurrency casinos can be significant as discussed earlier. Elliptic published a report in 2020 detailing red flags linked to crypto casinos:

---

[37] Sally Gainsbury et al., "*Migration from social casino games to gambling: Motivations and characteristics of gamers who gamble"*,ScienceDirect, October 2016 https://www.sciencedirect.com/science/article/pii/S074756321630348X

[38] Wesley Yin-Poole, "*Now Belgium declares loot boxes gambling and therefore illegal",* Eurogamer, April 2018. https://www.eurogamer.net/articles/2018-04-25-now-belgium-declares-loot-boxes-gambling-and-therefore-illegal

[39]Alex Matthews-King, "*Games like Fortnite use 'predatory' gambling techniques to make children spend, experts warn"*, Independent, June 2018 https://www.independent.co.uk/news/health/fornite-loot-llamas-payments-upgrades-items-gambling-addiction-a8421201.html

[40] Gambling Supervision Committee, "*AML/CFT Guidance for Virtual Currencies 2020"* Isle of Man, 2020 https://www.gov.im/media/1371388/vc-aml-guidance-2020.pdf

- Use of unlicensed, unregulated, or Tor-based gambling
- Regular use of online gambling sites such as Seals with Clubs that do not require any KYC, and make an open commitment to protecting anonymity of users
- Gambling sites that do not publish information about their ownership or their jurisdiction of registration
- Gambling sites that do not impose limits on volumes and values of cryptoasset used
- Funds are sent to mixers immediately before or after funds are deposited, or withdrawn at gambling sites.[41]

3. Blockchain Gaming

Non-fungible tokens (NFT) games are also gaining prominence like Axie Infinity where the Philippines was recently considering classifying the game as a payment system.[42] Over 40% of Axie players are from the Philippines according to the article that are able to earn a living wage from playing the game. The Vietnamese company Sky Mavis created the game to allow players to earn in-game cryptocurrency, which can then be traded and exchanged for real-world fiat currency. "*If the central bank determines Axie Infinity players use game tokens or AXS tokens as a payment method for a purchase, it could require the parent company to register with the central bank as an OPS (operator of payment systems). If the company is determined to be an OPS (operator of payment systems) and refuses to register, it risks being shut down."*[43]

Conclusions

Multiple AML/CFT vulnerabilities exist linked to online casinos if the proper oversight and guidance is not in place. The online casino market has matured significantly since its early days, however, there are still a number of jurisdictions with weaker regulatory approaches. The current shift in regulatory practices from Point of Establishment ("POE") to Point of Consumption ("POC") shows how onshore jurisdictions are now playing a much more active role where online casino operators are offering their services. Some of the key learning points include:

1. **Key AML vulnerabilities and mitigation**: The most significant AML vulnerabilities identified specific to online casino operators include non-face-to-face transactions, the potential for third party transactions, the difficulty in verifying source of funds, the beneficial ownership of the casino and/or payment provider, and inadequate CDD policy implementation by the casino operator. These vulnerabilities can be mitigated by a number of internal controls, policies and procedures. It is important that a thorough risk assessment is conducted by online operators to ensure risks are appropriately mitigated. These risk assessments should consider internal controls, licensing and integrity risks, customer, product and payment risks in their assessment.

2. **Payment methods:** should be appropriately regulated if they are offered as part of the online gambling process. Appropriate AML checks should be conducted by both the online casino and the payment provider linked to gambling payments. Consideration should be given to e-wallet services that may act as an intermediary payment provider between depositing cryptocurrency and gambling which could heighten AML vulnerabilities. In

[41] Elliptic, "*Financial Crime Typologies in Cryptoassets"*, 2020 Edition. (Charles McFarland, et. al., Jackpot! Money Laundering Through Online Casinos, McAfee
Labs White Paper, April 2014 p. 11.
[42] Ningwei Qin, "*Philippines may classify Axie Infinity as a company running a payment system*", Forkast, August, 2021 https://forkast.news/headlines/philippines-cbank-considers-classifying-axie-infinity-as-payment-system-operator/
[43] Ningwei Qin, "*Philippines may classify Axie Infinity as a company running a payment system*", Forkast, August, 2021 https://forkast.news/headlines/philippines-cbank-considers-classifying-axie-infinity-as-payment-system-operator/

addition, online operators should consider only regulated payment methods that have robust AML checks and avoid accepting payments from anonymous sources.

3. **Enforcement and Administrative Sanctions:** Gaming regulators have a number of enforcement tools available to ensure online operators are complying with relevant AML/CFT standards. These can include revoking or suspending the gaming license, cautioning the casino and requiring remedial actions to be undertaken along with fines and penalties. There must also be active coordination among regulators and law enforcement agencies to combat illegal operators and other illicit activity that may be present. Regulators should also conduct regular checks on licenced operators to ensure they are complying with the appropriate laws and regulations. Enforcement tools should be actively be applied in cases of non-compliance.

4. **The online casino simulation still showed gaps:** With both casinos "sampled," there were still significant red flags and gaps allowing anonymous payment methods and no requirements to obtain documentation linked to the source of funds. Regulators should ensure that all licenced operators are aware of their AML responsibilities and ensure adequate guidance and training is available to remediate any gaps. Enforcement actions and administrative fines should be actively used in cases of non-compliance and repeat non-compliance.

5. **Regulatory standards can vary by jurisdiction:** There are still white, grey and black-market operators when choosing to gamble online. AML vulnerabilities are particularly high for black and grey market operators where criminal groups may infiltrate and utilise these channels to launder illicit funds. Well-regulated jurisdictions and the shift in regulatory practices to "point of consumption" has assisted to better regulate online gambling markets especially across Europe. Other jurisdictions for online gambling have not been as successful in applying this approach as yet.

6. **Advances in technology:** Technology is playing a key role in advancing online gambling with accessibility levels significantly increasing with the use of apps. Social gaming, the use of cryptocurrency and blockchain gaming all come with potential AML risks that should also be considered as the gambling landscape advances.

Appendix 1: Overview of Selected Gaming Regulators

Countries of interest that do include have a gaming regulator include:	
Antigua and Barbuda	The **Antigua & Barbuda Gambling Authority** was set up as a result of new legislation in 2016, prior to this, casinos were regulated by the Financial Services Regulatory Commission ("FSRC"). They report that all internet gaming companies are classified as financial institutions and are subject to AML requirements.
Alderney (Guernsey)	The Alderney Gaming Control Commission (AGCC) regulates online casinos and other games of chance. Online casinos in Alderney developed from the operations of telephone bookmaking (the first licence being issued in 1997) which had been established earlier to take advantage of local rates of duty and taxation. As 31 December 2021 there were 20 online casinos, 11 of which also operate platforms.
Curacao (Netherlands)	The **Curacao Gaming Control Board** is the oversight authority. The country outsources licencing to four key providers known as Master Licences[44] that then provide sub-licences to gaming operators. There is no obligation to use software from a licensed provider in Curacao.[45]
Gibraltar	The Gibraltar Gambling Commissioner (GGC) has appointed the Gibraltar Regulatory Authority as the central oversight for online casinos. All gambling operations are governed by the Gambling Act 2005.[46] The Licensing Authority has traditionally only considered licensing blue chip companies with a proven track record in gambling in other jurisdictions. Nevertheless, the jurisdiction will also consider the licensing of appropriately funded start-ups and expanding operations proposing to relocate wholly or partly from other jurisdictions.[47] The gaming sector makes up around 25% of GDP.
Isle of Man (IoM)	The Gambling Supervision Commission (GSC) is the gaming oversight agency in the Isle of Man. Online gambling has been regulated since 2001 under the Online Gambling Regulation Act 2001. 45 active online operators with 4.3 million active players were reported at the end of 2018.[48] The IoM regulator has also been an early adopter of convertible virtual currencies. Gaming makes up almost 20% of the island's GDP.
Malta	The Malta Gaming Authority (MGA) was established in 2001 to regulate the online and land-based gambling markets. Online gaming is often referred to as remote gambling. Malta is home to some of the world's largest and most profitable online gaming companies and makes up around 10% of the

[44] Anyone wishing to acquire a Curacao gaming license will apply for what is formally known as a sublicense. The Curacao Ministry of Justice initially granted just four Online Gaming Master Licenses. These four license holders: Cyberluck Curacao N.V. #1668/JAZ, Gaming Services Provider N.V. #365/JAZ, Curacao Interactive Licensing N.V. #5536/JAZ and Antillephone NV #8048/JAZ[44]
[45] Lawstrust Website https://lawstrust.com/en/licence/gambling/b2b
[46] Gibraltar Remote Gambling ttps://www.gibraltar.gov.gi/finance-gaming-and-regulations/remote-gambling
[47] https://www.gibraltar.gov.gi/finance-gaming-and-regulations/remote-gambling
[48] Isle of Man – National Risk Assessment 2020 https://www.gov.im/media/1367979/isle-of-man-national-risk-assessment-2020-updated-140120.pdf

	country GDP.
Philippines	There are multiple gambling regulators in the Philippines including PAGCOR, Cagayan Economic Zone Authority (CEZA), Aurora Pacific Economic Zone and Freeport Authority (APECO) and Authority of the Freeport Area of Bataan (AFAB). The Philippines Offshore Gaming Operator (POGO) licencing regime has reported a decline in registration numbers due to increasing regulatory oversight, negative media linked to organised crime and the impending introduction of new taxes on gaming operators.
United Kingdom	The UK Gambling Commission is a non-departmental public body set up under the Gambling Act 2005. It regulates all commercial gaming in Great Britain, including all casinos, bingo, gaming machines and lotteries, including the National Lottery, betting and remote gambling. The Gambling Commission is the AML supervisory authority for 217 land-based and remote casinos, and the money service businesses offered in approximately 50 of those. Powers under the Gambling Act also afford the Gambling Commission the ability to revoke personal and business licences implement unlimited fines for breaches and add additional licence conditions for businesses to operate.[49] The Gambling Commission also supervises MSBs in casinos.

[49] The UK National Risk Assessment (2020) https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/945411/NRA_2020_v1.2_FOR_PUBLICATION.pdf

Appendix 2: AML Red flag indicators for online casino operators[50]

- Information provided by the player contains a number of mismatches (e.g., email domain, telephone or postcode details do not correspond to the country)
- The registered credit card or bank account details do not match the player's registration details
- The player is situated in a higher-risk jurisdiction or is identified as being listed on an international sanctions list
- The player is identified as a politically exposed person
- The player seeks to open multiple accounts under the same name
- The player opens several accounts under different names using the same IP address
- The withdrawals from the account are not commensurate with the conduct of the account, such as for instance where the player makes numerous withdrawals without engaging in significant gambling activity
- The player deposits large amounts of funds into his online gambling account
- The source of funds being deposited into the account appears to be suspicious and it is not possible to verify the origin of the funds
- The customer logs on to the account from multiple countries
- A deposit of substantial funds followed by very limited activity
- The player has links to previously investigated accounts
- Different players are identified as sharing bank accounts from which deposits or withdrawals are made.

[50] Source: Moneyval Report