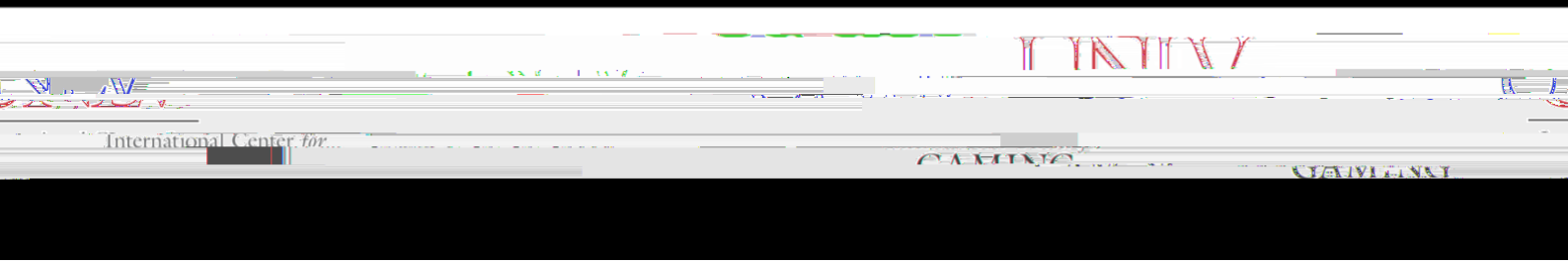


Online Casinos, Alternative Payment Mechanisms

Methodology.....5
Executive Summary.....4

Section 1: The rise of online casinos & alternative payments.....5

The history of law enforcement actions against online gambling operators.....6

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.

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" 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 a9 (ort)6(l)7 nk accouTis nec

Section 2: Online payments & the associated AML vulnerabilities

The proliferation of alternative online payment methods

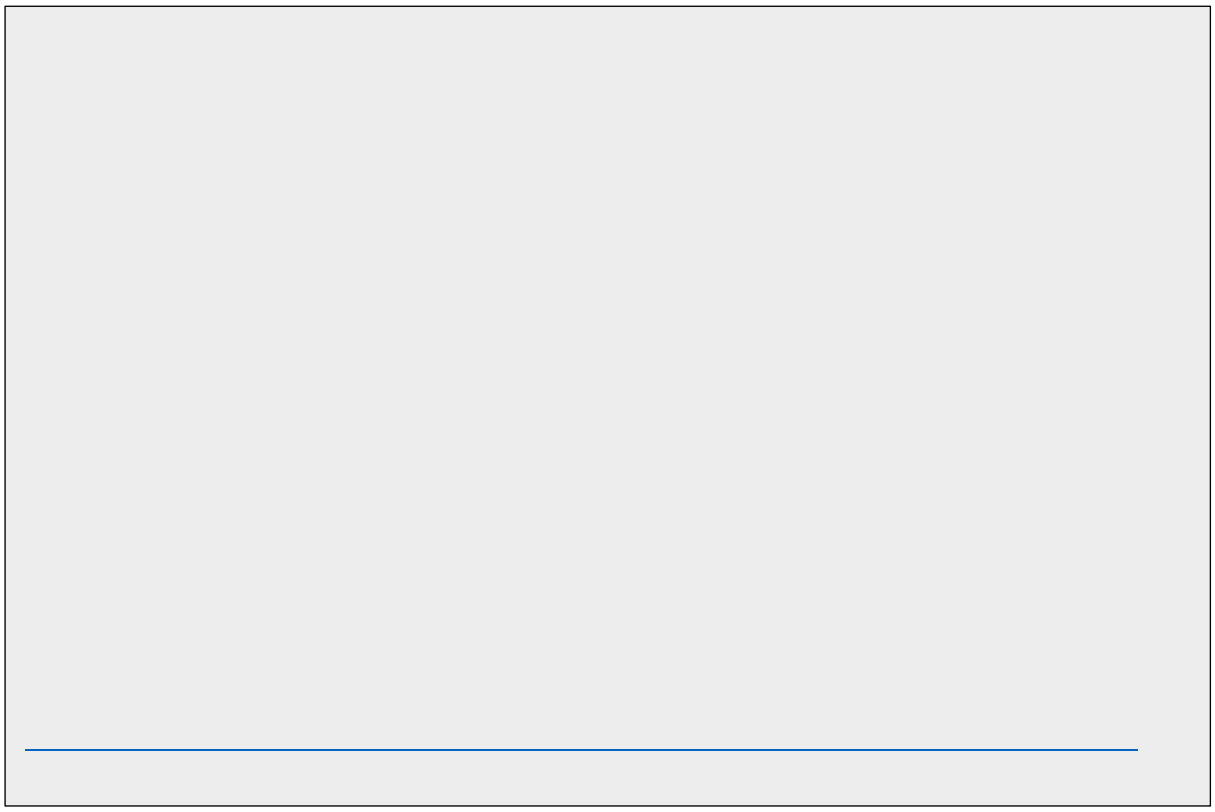
Traditional payment methods can include bank transfers, credit cards, cheques, and money remittances. Alternative payment systems are newer innovative payment methods such as e-wallets, pre-paid cards, online third-party payment providers (i.e.: Paypal), and cryptocurrencies.

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



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 andL (i)7 n.

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 fund 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")

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 on-line: 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 load1 (p)-20 (aa)7 7 (bl)7 ((h)-20

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

Section 3: Regy51020 ((298d [( )-5)5 (e)1772.9 ( )-72k an)5 (d63 0. (on) (on)5

Date and Location	Breaches/Fines
2017 (UK) Social Responsibility Breaches	The UK Gambling Commission fined 888 Holdings £7.8m for is.6-[. (a)>Bndean9EMCports.6-[.5620(vM1.7s)176.1 Tm (35 15 > ( )-35 (t

- Use of unlicensed, unregulated, or [illegible]-based gambling
- Regular use of online gambling sites such as Sealswap 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

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