Gambling and Gaming Good practices for Payment Institutions

DeNederlandscheBank
EUROSYSTEEM

Disclaimer

This good practices document provides non-binding recommendations on the application of the Financial Supervision Act (*Wet op het financieel toezicht – Wft*) and the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft*) to payment institutions serving merchants in the gambling and gaming sector. It sets out our expectations regarding observed or expected behaviour in policy practice that reflects an appropriate application of the rules to which this good practices document pertains.

We encourage payment institution serving merchants in the gambling and gaming sector to take our expectations into account in their considerations and decision-making, without being obliged to do so, while also taking into consideration their own specific circumstances. The good practices document is only indicative in nature, and therefore does not alter the fact that some payment institutions should apply the underlying regulations differently, and possibly more strictly. It is the institutions' responsibility to take this into account.

Introduction

With this good practices document, De Nederlandsche Bank N.V. (DNB) aims to provide payment institutions[1] with guidance on how to manage risks related to the provision of services to remote gambling providers (online gambling websites)[2] and providers of online gaming websites, collectively referred to below as the **gambling and gaming** sector.

In 2021, we conducted a thematic examination into payment institutions offering payment services to merchants in the gambling and gaming sector. We selected nine payment institutions that serve merchants operating in the gaming and/or gambling sector for the examination. In particular, we focused on the controls payment institutions had implemented with regard to their service provision to merchants in the gambling and gaming sector. Subsequently, several payment institutions were selected for a desk-based, in-depth investigation.

Risk management always requires customisation. This also applies to the risks associated with gambling and gaming. The examples presented in this good practices document will often, but not always, be directly applicable to every single institution.

Relevant laws and regulations

Among other requirements, payment institutions must comply with the following statutory obligations to mitigate money laundering and terrorist financing risks. This good practices document provides non-binding suggestions for meeting these obligations.

- Sound and ethical operational management (Section 3:10 read in conjunction with Section 3:17 of the Financial Supervision Act (*Wet op het financieel toezicht – Wft*) and with Sections 10 and 17 of the Decree on Prudential Rules for Financial Undertakings (*Besluit prudentiële regels Wft - Bpr*);
- Measures to identify and assess money laundering and terrorist financing risks through the SIRA (Section 2b of the Anti-Money Laundering and Anti-Terrorist Financing Act (*Wet ter voorkoming van witwassen en financieren van terrorisme – Wwft*)
- Policies, procedures and measures to minimise and effectively manage the risks of money laundering and terrorist financing, as well as the risks identified in the most recent versions of the supranational and national risk assessments (SNRA and NRA) (Section 2c of the *Wwft*)
- Customer due diligence (Sections 3, 8 and 9 of the *Wwft)*
- Transaction monitoring (Sections 2a and 3(2), opening words and under d, of the *Wwft*
- Reporting unusual transactions (Section 16 of the *Wwft*)

1 This good practices document could also be relevant for other payment service providers.
2 From 1 October 2021, a provider of online gambling is required to apply for an operating licence under Section 31a of the Betting and Gaming Act. A licensed provider is supervised by the Kansspelautoriteit.

Contents

Integrity risks in the gambling and gaming sector

Gambling carries an increased inherent risk of money laundering and terrorist financing.[3] Examples of risks related to the nature of the service include the sheer number of transactions, the amount of the transactions and the speed of circulation of the money involved. Gaming also carries a risk of money laundering. The Anti Money Laundering Centre has cited a number of examples regarding the risk of money laundering[4] in the gambling and gaming sector.[5]

Gambling

Gambling involves the risk of money laundering. The origin of money can be hidden, using illegal money as pay-ins and laundering it through a gambling platform. The following examples illustrate how this can be done through online gambling:

- Players use anonymous payment methods, such as credit and debit cards, prepaid cards, cheques and cryptocurrencies, to feed pay-ins into gambling accounts. Only illegal providers facilitate this.
- Money is moved from a payment account to a gambling account.[6] The money is then wagered and any winnings are received. These are paid out to the gambling account and transferred back into a payment account. This description assumes that a player does not use their own money to play, or hardly at all.
- Players can arrange for one player to lose intentionally for the benefit of the other player. The money is then paid out to the winning player's gambling account.
- A gambling account can be used to pay for illegal transactions. For example, money can be moved in a player-to-player transfer without actually playing. The seller then arranges for the money to be paid from their gaming account to their payment account. The proceeds are not gambling winnings but, for example, income from the sale of goods. Only illegal providers facilitate this.
- Players can use a gambling account to store and hide money from the authorities.

3 EBA Guidelines EBA/GL/2021/02, 1 March 2021, guidelines 9.6, 10 4 and 12.5
4 Lotteries pose a low money laundering risk https://www.rijksoverheid.nl/documenten/kamerstukken/2021/01/27/bijlage-1-vervolgonderzoek-naar-risicos-witwassen-en-terrorismefinanciering-bij-aanbieders-in-de-kansspelsector-die-vrijgesteld-worden-van-de-verplichtingen-van-de-wwft.
5 Online gokken als witwasmethodiek - AMLC Online games en witwassen - AMLC
6 Fraud involving player credits may also prompt a gaming operator to report an incident pursuant to the Policy Rules of the Board of Directors of the Kansspelautoriteit on the reporting duties of licence holders.

Gaming

Gaming also involves the risk of money laundering. The large amounts of money involved in the online gaming world make this market attractive to criminals. In online gaming, recreational aspects are more important than making money. In-game currencies play an important role in online games. Among other things, they enable players to gain access to higher levels and purchase game items. Also referred to as non-convertible virtual currencies, they can be earned by completing missions or be purchased.[7]

- There are several online exchange platforms (Real Money Trading) on which virtual currencies or items can be exchanged or traded for money.
- Online currencies are increasingly being traded using anonymous payment methods.
- Money can be laundered or stolen in various ways. For example, criminals can gain access to a computer and a player's data through phishing and hacking.
  - The player's bank account linked to the gaming account can be drained by purchasing game items and selling them on exchange platforms.
  - The account can be used to transfer illicit funds. In addition, criminals can duplicate virtual currencies and game items and sell them repeatedly or develop and operate games themselves.

7 https://www.fatf-gafi.org/media/fatf/documents/reports/virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf

Gambling and gaming risks for payment institutions

The flows of funds of gambling and gaming merchants pass through the accounts provided by payment institutions, which means they are expected to adequately manage the associated risks. The payment institutions thus act as gatekeepers.

Our thematic examination looked at both the gambling and gaming sectors. In practice, the distinction between these sectors is often blurred. Gaming merchants can have certain features that are reminiscent of gambling (e.g. an element of chance). In such cases, different risks arise than when it only concerns gaming. The related customer due diligence and transaction monitoring may require different elements for gambling and gaming merchants, and must be adapted accordingly.
We wish to stress that payment institutions are expected to distinguish clearly between gambling and gaming merchants and report them as such in their annual integrity risk assessment (IRAP).

SIRA

Pursuant to Section 2b of the *Wwft*, payment institutions must take measures to identify and assess money laundering and terrorist financing risks. Payment institutions serving customers in the gambling and gaming sector are expected to provide insight into the risks associated with both sectors in their systematic integrity risk analysis (SIRA), for example by including scenarios that address sector-specific risks. Examples include:

- AML/CTF scenarios relating to risks linked to the provision of services in the high-risk gambling and gaming sector

Example scenarios:

- The paying institution is not able or is insufficiently able to determine whether pay-outs by the gambling merchant exceed the thresholds set.
- The risk of virtual game items being purchased with illicit money. These items can have an economic value outside the game.

- AML/CTF scenarios relating to risks linked to servicing merchants in high-risk jurisdictions and/or with complex structures, which is a common feature among gambling and gaming merchants

- AML/CTF scenarios related to risks linked to payment flows and payment methods

Example scenarios:

- Customer pay-ins in the gambling sector are disproportionate to pay-outs made to customers, creating the risk of money laundering.

- The use of different, often anonymous, payment methods increases the risk of money laundering in the gambling and gaming sector.

- Scenarios related to risks linked to the regulation of merchants

Example scenarios:

- The payment institution provides services and/or products to gambling merchants that are not licensed in the country where they conduct their activities, thus creating a risk that the services or products will be used for a different purpose.[8]
- The payment institution provides services and/or products to gambling merchants that use them for criminal purposes or to target children.

We provide guidance on the SIRA in our English-language publication Integrity risk analysis – more where necessary, less where possible.

8 The operators and brand names they use can be looked up on the Kansspelautoriteit's website to check whether they are licensed.

Policy and customer due diligence

Pursuant to Section 2c of the *Wwft*, payment institutions have adopted policies to manage money laundering and terrorist financing risks. To put this policy into practice regarding gambling and gaming merchants, payment institutions can consider the following elements, which relate to customer due diligence pursuant to Sections 3, 8 and 9 of the Wwft.

We provide guidance on customer due diligence in our English-language publication in our Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act.

Good practices:

A payment institution has adopted a gambling and gaming policy. The following elements could be considered for inclusion in the policy:

- The payment institution establishes where the merchant operates, i.e. in which jurisdiction if offers the online gambling and gaming services, and for what purpose the payment products will be used. It does so to determine whether the payment products will be used only on the gambling and gaming market.
- The institution conducts (further) investigations if it suspects that the merchant is offering illegal (i.e. unlicensed) gambling services. This allows the institution to rule out the possibility that the service is misused for the illegal provision of online gambling services. When regulatory changes occur, e.g. a merchant's licence is revoked or has expired, the payment institution acts promptly, for example by blocking pay-ins and pay-outs.
- The payment institution requests a merchant's licence from time to time, checking it against the licence registers or other sources. The gambling licence is used to check whether the jurisdictions where gambling is offered fall within its geographical scope. The institution also checks whether the gambling offered via the website, app, etc. fall within the scope of the gambling licence.
- The institution requests the merchant's AML/CTF policy and procedures and checks whether the merchant has implemented controls to manage ML/TF risks. See the Kansspelautoriteit's Wwft guidance document for the gaming sector.
- The payment institution audits or checks the merchant for compliance with the Wwft.
- Depending on the merchant's risk classification, the institution conducts annual reviews of gambling and gaming merchants.
- Approval must be obtained from senior management upon customer acceptance and after each review for gambling and gaming merchants.

Transaction monitoring

Pursuant to Sections 2a and 3(2), opening words and under (d), of the *Wwft*, payment institutions that serve merchants in the gambling and gaming sector are expected to adequately monitor the merchants' transactions. This may involve applying specific business rules for transactions involving merchants active in gambling and gaming. To do so, it is important that merchants in the gambling and gaming sector are assigned the right risk classification and merchant category code. Failing this, merchants are analysed using the wrong business rules (thresholds), resulting in unusual transactions going undetected.[9]

Good practices:

For gambling and gaming merchants, certain thresholds may be set as part of the payment institution's transaction monitoring. Examples of such thresholds are given below.

- Amounts and frequency for pay-ins, pay-outs, or both (specify thresholds). For example, a single transaction from a gambling merchant of €15,000 or more within 24 hours. Also, a threshold could be set defining a certain percentage by which a transaction exceeds the average amount for the past six months, which will detect a change in transaction pattern at the merchant level.
- Comparing pay-ins and pay-outs. The pay-outs made by a payer (the merchant's customer) could be compared with the same payer's pay-ins (in case it is possible to establish thresholds at the payer level). If a pay-in differs from the pay-out by a certain set percentage, the payment institution investigates the transaction.
- The payment method used for pay-ins and/or pay-outs. If an anonymous payment method is used, a transaction could be investigated if a certain threshold is exceeded.
- Besides using thresholds, other business rules may be created. Examples include checks related to:
  - The use of corporate accounts involving legal entities to make pay-ins and pay-outs.
  - IP addresses. This includes, for example, payments made to and from the same IP address and payments in which shopper's jurisdiction differs from that of the IP address.
  - Involvement of high-risk jurisdictions. Incoming transactions from high-risk jurisdictions could be checked.

9 If payment service providers detect fraud in the purchase of player credits, this could be indicative of money laundering and/or terrorist financing. The payment service provider must report such unusual transactions to the Financial Intelligence Unit-the Netherlands (FIU-NL).

- Transaction checks (pay-in/pay-out) for illegal gambling. This may include blocking transactions from the payer and transactions to the payee in jurisdictions where merchants are not licensed for gambling activities or where these services are prohibited.

We provide guidance on customer due diligence in our English-language publication in our Guideline on the Anti-Money Laundering and Anti-Terrorist Financing Act and the Sanctions Act.

DeNederlandscheBank

EUROSYSTEEM

De Nederlandsche Bank N.V.
Postbus 98, 1000 AB Amsterdam
020 524 91 11
dnb.nl/en