22 February 2022

D E C I S I O N

Trustly Group AB
via the Chairman of the Board of Directors
Rådmansgatan 40
SE-113 57 Stockholm Sweden

FI Ref. 20-20967
Notification No. 1

Finansinspektionen
Box 7821
SE-103 97 Stockholm Sweden
[Brunnsgatan 3]
Tel +46 8 408 980 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

This translation is furnished solely for information purposes. Only the version of the decision in Swedish applies for the application of the law.

Warning, administrative fine and injunction

Finansinspektionen's decision (to be announced on 22 February 2022 at 12:00 p.m.)

1. Finansinspektionen is issuing a warning to Trustly Group AB (556754-8655).

   (Chapter 8 Section 8 of the Payment Services Act [2010:751])

2. Trustly Group AB must pay an administrative fine of SEK 130,000,000.

   (Chapter 8 Section 14 of the Payment Services Act)

3. Finansinspektionen issues an injunction to Trustly Group AB that by 30 November 2022 it must treat the natural persons that enter into a contractual agreement with Trustly in order to make a payment and when doing so approve the company's general terms and conditions as customers pursuant to the Act on Measures against Money Laundering and Terrorist Financing (2017:630).

   (Chapter 8 Section 8 of the Payment Services Act)

4. Trustly Group AB must report in writing to Finansinspektionen by 4 January 2023 the measures the company has applied as a result of this injunction pursuant to point 3 and the way in which these measures have resulted in compliance with the injunction.

To appeal the decision, see *Appendix 1*.

Summary

Trustly Group AB ('Trustly' or 'the company') is a payment institution that is authorised to provide payment services pursuant to the Payment Services Act (2010:751). The company provides, inter alia, an pay-in service. It has described this service as a combination of a payment initiation service and money remittance, where the payment initiation constitutes the first step in the money remittance. The company also has an pay-out service, which it has described as money remittance. Trustly refers to the natural persons who use the pay-in and pay-out services as 'end users'.

Finansinspektionen has investigated Trustly's compliance with the Act on Measures against Money Laundering and Terrorist Financing (2017:630) and Finansinspektionen's Regulations (FFFS 2017:11) regarding Measures against Money Laundering and Terrorist Financing with regard to the rules on the general risk assessment, risk assessment of customers, procedures and guidelines, and customer due diligence measures, as well as monitoring and reporting. This investigation has mostly been limited to the company's operations that are linked to the gambling industry.

The gambling industry is the company's largest business area. In terms of transaction volumes, transactions to and from the gambling industry during the investigation period accounted for more than half of the company's total transaction volume. Finansinspektionen can therefore state that the company has high exposure to an industry that presents a high risk of money laundering and terrorist financing.

Finansinspektionen's investigation has revealed a number of deficiencies in central parts of the money laundering regulatory framework, as the company has not treated the company's end users as customers pursuant to the Money Laundering Act. Finansinspektionen has found that Trustly has thereby failed to include a large proportion of the company's customers in its measures to prevent money laundering and terrorist financing. In violation of the Money Laundering Act, Trustly has not included these customers in its general risk assessment nor in the company's procedures and guidelines. As far as these customers are concerned, the company has not carried out a risk assessment of them either, it has not applied customer due diligence measures for them and has not monitored them as customers.

As well as the deficiencies relating to the company not correctly defining who constitutes a customer of the company under the Money Laundering Act, the investigation has also shown that the company has not complied in other respects with central rules in the money laundering regulatory framework that relate to the general risk assessment, risk assessment of customers, procedures and guidelines for customer due diligence, customer due diligence measures and monitoring.

These deficiencies primarily relate to an industry that presents a high risk of money laundering and terrorist financing, and in light of Trustly's role in the payment chain, the company has adopted a position that can almost be compared to being a hub between the banks and the gambling companies. There has therefore been a high risk of Trustly and the financial system being used for money laundering and terrorist financing. Overall, Finansinspektionen assesses that the deficiencies have been of such a nature that there are grounds to intervene against Trustly.

The violations resulting from Trustly not treating end users as customers pursuant to the Money Laundering Act need to be handled separately from the other violations. Although there are several circumstances that would suggest that the violations should be considered serious, the circumstances in this section are such that the company, following an investigation previously carried out by Finansinspektionen, bears a lesser degree of responsibility than would otherwise have been the case. In this section, Trustly is therefore ordered to take measures to rectify the situation.

Regardless of the deficiencies that relate to Trustly not treating end users as customers pursuant to the Money Laundering Act, Finansinspektionen considers that the other deficiencies set out in its decision are serious, which is why there are grounds to consider revoking Trustly's authorisation. In light of the information provided by the company on measures that it has applied or is planning to apply, Finansinspektionen's assessment is that the prospect of Trustly rectifying the deficiencies and complying with the regulations in the future is so good that a warning for Trustly will be sufficient for this section. The warning is accompanied by an administrative fine of SEK 130,000,000.

Table of Contents

1 Background

1.1 The company and its operations

Trustly Group AB ('Trustly' or the 'company') is a Swedish payment institution that is authorised to provide payment services under the Payment Services Act (2010:751). The company was founded in 2008 and provides payment solutions through its direct payment technology. In terms of turnover, number of employees and payment volume, Trustly is one of the largest payment institutions in Sweden. The company has four main business areas: the gambling industry[1], e-commerce, financial services and travel services. The gambling industry accounts for more than half of the company's transaction volume[2] and a significant proportion of both the number of payment service users and the number of corporate customers.

As a payment institution, Trustly offers, inter alia, pay-in and pay-out services. Trustly's main service, *the pay-in service*, is a payment method that enables a private individual to make a payment or a transfer from their bank account to the payee's account. According to the company's description of this service, it enables payments to be made more quickly than using other payment methods. Trustly has client accounts in several banks to enable it to provide this service. When a private individual makes a payment through the company's service, the money is transferred from the person's bank account to one of the company's client accounts at the same bank. Trustly then forwards the amount to the recipient's account at a predetermined interval. The company has explained that this service can be viewed as a combination of a payment initiation service and money remittance, where the payment initiation constitutes the first step in the money remittance.

Trustly's *pay-out service* is a payment method through which an e-commerce company can make a refund to a private individual, or alternatively a payment method through which a private individual can request, for example, that a gambling company executes a transfer from the private individual's gambling account at the gambling company to the private individual's bank account. When using this service, the transaction goes through Trustly's client accounts as well. The company has stated that the pay-out service constitutes money remittance.

As well as the company's pay-in and pay-out services, the company provides an account information service and a direct debit service.

The company refers to the natural persons who use the company's pay-in and pay-out services as *end users*. The people who use the company's direct debit service are referred to as *direct debit customers*. These are the definitions that have been used for these groups in this decision.

[1] The gambling industry here refers to commercial online gambling, such as betting or casino operations.
[2] Transaction volume refers to the total sum of the payments made through the company.

According to its most recently adopted annual report for the 2020 financial year, Trustly reported a net turnover of SEK 1,752,029,000 and a balance sheet total of SEK 1,801,689,000. The company reported that it had 306 employees in Sweden in 2020.

1.2 The case

In October 2020, Finansinspektionen opened an investigation into Trustly's compliance with the Act on Measures against Money Laundering and Terrorist Financing (2017:630) (Money Laundering Act) and Finansinspektionen's Regulations (FFFS 2017:11) regarding Measures against Money Laundering and Terrorist Financing (Money Laundering Regulations). In this decision, the Money Laundering Act and the Money Laundering Regulations are jointly referred to as the money laundering regulatory framework.

This investigation was limited to cover Trustly's general risk assessment, risk assessment of customers, procedures and guidelines, and customer due diligence measures, as well as its monitoring and reporting. Apart from the general risk assessment, this investigation is limited to the company's operations that are linked to the gambling industry due to the elevated risk of money laundering and terrorist financing associated with this industry and the company's high exposure to this industry.[3]

Finansinspektionen carried out a digital on-site visit to Trustly on 4 November 2020. Subsequently, on 2 December 2020, the authority interviewed the person who was responsible at the time for the company's unit for preventing money laundering and terrorist financing.

Finansinspektionen sent a verification letter to Trustly on 19 April 2021, in which the authority presented its observations and preliminary assessments. The company's response to the verification letter was received by the authority on 25 May 2021. Finansinspektionen then had a meeting with Trustly at the company's request. At this meeting, Trustly gave an update of its work on the action plan that the company had submitted in its response to the verification letter.

When the case had been submitted for a sanction assessment, Finansinspektionen sent a request for a statement to Trustly on 28 September 2021. The company was thus given the opportunity once again to submit a statement not only on Finansinspektionen's observations and preliminary assessments, but also on the authority's considerations to intervene against the company. Trustly submitted its statement to Finansinspektionen on 1 November 2021. The company

[3] Both national and international sources have assessed that the gambling industry presents a high risk of money laundering and terrorist financing: see, for example, the Swedish Gambling Authority's risk assessment from 2020, p. 21, the Financial Intelligence Unit of the Swedish Police's Annual Report for 2020, p. 9 and the appendix to the EU Supranational Risk Assessment in 2019, p. 220.

subsequently submitted updates regarding its work on the measures on 12 November, 22 November, 30 December 2021, 3 February 2022 and 11 February 2022.

1.3 The scope of the investigation

The investigation refers to the period from 1 January 2020 to 31 August 2020 ('the investigation period') and has been carried out by Finansinspektionen requesting material from Trustly for this period. Unless otherwise stated, the observations in this decision apply to all versions of the documents that the company has submitted and that have been valid during the investigation period.

As part of its investigation, Finansinspektionen has requested and examined Trustly's general risk assessment and related appendices, the company's risk assessment of customers, procedures and guidelines for customer due diligence measures, procedures and guidelines for monitoring continuous business relationships and documentation describing the company's monitoring system, the scenarios used, as well as the company's procedures and guidelines for reporting suspicious transactions or activities to the Financial Intelligence Unit. When examining the company's monitoring, Finansinspektionen also requested the company's procedures for model risk management and a report on the results of the most recent validation of this model.

Finansinspektionen has requested and examined the company's business plan and its related appendices as well.

Finansinspektionen has also examined the customer due diligence measures that Trustly has taken for 50 private individuals and nine gambling companies. The 50 private individuals were broken down into 22 direct debit customers and 28 end users. In terms of private individuals, Finansinspektionen has taken its sample from a list of the private individuals who transferred the largest combined value during the period to gambling companies and the private individuals who Trustly reported most often to the Financial Intelligence Unit during the period for suspicious transactions or activities linked to gambling companies. In terms of gambling companies, Finansinspektionen has taken its sample from a list of gambling companies with which Trustly had business relationships and that transferred the largest combined value to and from private individuals with a Swedish bank account through Trustly during the investigation period. The terms 'corporate customer' and 'gambling company' are used synonymously in this document.

Finansinspektionen has also examined ten alerts in Trustly's system for monitoring transactions and the investigative measures that the company has applied as a result of these alerts. The sample for this has been based on alerts that were generated for the private individuals who had the largest combined value of transactions to and from gambling companies during the investigation period.

Finansinspektionen has found grounds to move forward with the part of this investigation that relates to Trustly's general risk assessment, risk classification of customers, procedures and guidelines, customer due diligence measures and transaction monitoring in the sanctions assessment. Anything else that has emerged as part of this investigation has not justified any action on the part of Finansinspektionen.

2 Applicable provisions

In its decision, Finansinspektionen has applied provisions from the Money Laundering Act, the Money Laundering Regulations and the Payment Services Act.

A more detailed description of these provisions is set out in *Appendix 2*. Section 5 presents the applicable provisions for the intervention in greater detail.

3 Starting points

3.1 Money laundering regulatory framework

Trustly comes under the term *obliged entity* in the Money Laundering Act and under the term *company* in the Money Laundering Regulations. For clarity of presentation, the provisions that apply for a payment institution under the money laundering regulatory framework will be given, even if these provisions also apply to other obliged entities and companies.

Money laundering is a criminal activity where perpetrators use payment institutions and other companies to make illegal proceeds available for consumption and investments.

The money laundering regulatory framework aims to prevent, inter alia, financial companies from being used for money laundering and terrorist financing. Consequently, a payment institution has to assess and manage the risks of the services provided by the institution being used for money laundering and terrorist financing. If the institution does not do this, it may not only create an opportunity for criminals to launder money, but also a lack of trust in the institution and the Swedish payment services market. In the long run, this could result in a lack of trust in the Swedish financial market as a whole, both among Swedish consumers and among actors in other countries that do business with or through Swedish financial companies.

The money laundering regulatory framework adopts a risk-based approach. This means that a payment institution must apply measures that are proportionate to the risks of money laundering and terrorist financing to which it is exposed. It also means that a payment institution has to identify its risks and allocate its resources to where the risks are the greatest.

3.2 The general risk assessment and the customer's risk profile

The Money Laundering Act states that in order for a payment institution to be able to manage its risks, it must assess how the products and services that it provides in its operations may be used for money laundering and terrorist financing, and the likelihood of this risk occurring (general risk assessment). In its assessment, the institution must consider in particular the customers and distribution channels that it has, as well as any geographical risk factors. The institution must therefore identify, understand and assess the risks associated with its own operations being used for money laundering or terrorist financing. The general risk assessment must be designed so that it can serve as a basis for the institution's procedures, guidelines and other measures to prevent money laundering. An inadequate general risk assessment has a negative impact on the way the individual institution prioritises its resources and designs its procedures for, inter alia, customer due diligence and transaction monitoring. These various steps are therefore linked to one another, so deficiencies in one could lead to deficiencies in another.

In addition to the institution's general risk assessment, the institution must also, pursuant to the Money Laundering Act, assess the risk associated with an individual customer and its business relationship (the customer's risk profile).

3.3 Procedures and guidelines

Pursuant to the Money Laundering Act, a payment institution must have documented procedures and guidelines in place for its customer due diligence measures, and monitoring and reporting, as well as for processing personal data. If the payment institution applies this risk-based approach, its procedures and guidelines are of great importance. In practice, the internal procedures largely replace such detailed provisions in acts or regulations that provide clear and detailed codes of practice (Government Bill 2016/17:173 p. 212). The payment institution must determine the scope and content of the procedures and guidelines based on the institution's size, nature and the risks of money laundering and terrorist financing that have been identified in the general risk assessment.

3.4 Customer due diligence measures

Pursuant to the Money Laundering Act, a payment institution must apply a number of specific measures to fulfil the customer due diligence requirements. However, the act does not specify in detail the scope of the customer due diligence measures that a payment institution has to apply. Instead, it is the individual institution that is responsible for determining the measures it deems appropriate in view of the identified risks, based on its general risk assessment.

The payment institution must adapt the measures to the risk of money laundering and terrorist financing that it assesses that a specific customer is exposed to. If this risk is assessed to be low to normal, the institution must apply basic

measures, and in some cases simplified measures may be sufficient. In cases where the risk of money laundering and terrorist financing is assessed as being high, the institution must apply enhanced customer due diligence measures. These measures must include much more extensive checks, assessments and investigations.

If a payment institution is to have good knowledge of its customers, it must apply customer due diligence measures when establishing a business relationship. The term *business relationship* denotes a commercial relationship that is expected at the time it is established to have a certain permanence. A business relationship can arise either the first time that the customer and the payment institution have contact with each other or later, through the actual actions of the parties (Government Bill 2016/17:173 pp. 189).

A payment institution may not establish or maintain a business relationship or carry out occasional transactions if the institution does not have sufficient knowledge of the customer to be able to manage the risk of money laundering that may be associated with the customer relationship. If a business relationship has not been established, a payment institution is still obliged to apply customer due diligence measures for occasional transactions that exceed specific thresholds that are stipulated in the act.

3.5 Monitoring

Pursuant to the Money Laundering Act, a payment institution must continuously monitor business relationships and transactions by checking and documenting that the transactions that are carried out are consistent with the institution's knowledge of this customer and its business and risk profile, in order to detect any activities and transactions that may be suspected as being involved in money laundering or terrorist financing. If suspicions remain following a more in-depth analysis, the institution must submit data without delay about all of the circumstances that could indicate money laundering or terrorist financing to the Financial Intelligence Unit of the Swedish Police.

3.6 The risk of Trustly being used for money laundering

The risk of money laundering and terrorist financing in payment institutions has been assessed as being significant.[4]

Trustly is a payment institution whose operations are largely targeted at the gambling industry. The gambling industry has been classified by several authorities as being at high risk of money laundering and terrorist financing.[5]

[4] *Nationell riskbedömning av penningtvätt och finansiering av terrorism i Sverige 2020/2021*, 2021, p. 65. An English version is available at www.polisen.se.
[5] See, for example, *Identifiering och bedömning av risker för penningtvätt på den svenska spelmarknaden*, Spelinspektionen (Swedish Gambling Authority), 2020 (an English translation is available at www.spelinspektionen.se); and *Nationell riskbedömning av penningtvätt och*

The main risks that characterise the gambling industry, particularly for online gambling, are a high turnover and a large number of transactions.[6] The Financial Intelligence Unit has also reported that the gambling industry is repeatedly used for money laundering and that some of the actors that launder money on the gambling market may be linked to criminal groups in vulnerable areas, especially with links to drug crime and violent crime.[7]

Trustly's general risk assessment states that the company has identified the gambling industry as presenting a high risk of money laundering and that the end users' transactions to and from the gambling industry constitute one of the company's main risk scenarios for money laundering. The general risk assessment also states that a significant proportion of all reports of suspicious activities and transactions that Trustly has sent to the Financial Intelligence Unit relate to the gambling industry.

In terms of transaction volume, transactions to and from the gambling industry during the investigation period comprised a significant proportion of Trustly's total transaction volume. During the investigation it has also emerged that transactions to and from gambling companies are almost exclusively carried out by private individuals. Finansinspektionen can therefore state that Trustly has a high exposure to an industry that presents a high risk of money laundering and that in particular the private individuals' transactions to and from gambling companies comprise a significant proportion of both its risk exposure and the company's operations.

Trustly's role in the payment chain means that the company has adopted a position that can almost be compared to being a hub between the banks and the gambling companies. The company's role therefore means that it is in a particularly good position to identify and prevent suspected money laundering or terrorist financing linked to transactions to and from the gambling industry. If Trustly does not take its full responsibility for this, there is a risk that it will have limited opportunities to prevent money laundering and terrorist financing.

As a result of Trustly's business model, which means, inter alia, that the company has focused specifically on the gambling industry and developed products and services specifically for this industry, Finansinspektionen assesses that the company has a significant risk exposure to the gambling industry. It is therefore Finansinspektionen's opinion that the risk-based approach requires the company to apply particularly strong measures to be able to manage the risk presented by the gambling industry to the company's operations.

---

finansiering av terrorism i Sverige 2020/2021, 2021, pp. 117 (an English translation is available at www.polisen.se).

[6] *Identifiering och bedömning av risker för penningtvätt på den svenska spelmarknaden*, Spelinspektionen (Swedish Gambling Authority), 2020, p. 21 (an English translation is available at www.spelinspektionen.se).

[7] *Finanspolisens årsrapport för 2020*, p. 9 (an English translation is available at www.polisen.se).

3.7 General information about Trustly's position

Trustly raised a number of objections in its response to the verification letter. In the statement that Trustly subsequently submitted to Finansinspektionen, the company has generally not contested the authority's observations and preliminary assessments, but instead presented the measures it has applied or plans to apply to rectify the deficiencies identified by Finansinspektionen. In this decision, Trustly's opinion on a matter is only reported to the extent that the company has presented its opinion in the statement.

4 Finansinspektionen's observations and assessments

4.1 Trustly's treatment of end users when applying the Money Laundering Act

4.1.1 The term 'customer' in the Money Laundering Act

Chapter 8 Section 8 (4) of the Money Laundering Act states that a *customer* is a person who has entered into or is about to enter into a contractual relationship with an obliged entity. According to point 1 of this paragraph, *business relationship* refers to a commercial relationship that is expected at the time it is established to have a certain permanence. If a person is to be considered a customer of an obliged entity, the requirement for permanence is not required for a business relationship to be considered to be established. The term 'customer' therefore covers both the persons that establish a business relationship with an obliged entity and those that enter into agreements of a more temporary nature, for example, in order to execute an occasional transaction with an obliged entity (Government Bill 2016/17:173 p. 188). The fact that a customer is also a customer of another obliged entity that is involved in the same transaction in some way or another does not exclude the customer being regarded as a customer of the first obliged entity as well.

The question as to who is to be considered to be a customer is of great importance when applying the Money Laundering Act. For example, when the payment institution performs its general risk assessment, it must pay special attention to the customers it has (Chapter 2 Section 1 second paragraph of the Money Laundering Act); and the institution may only execute an occasional transaction with a customer if the institution has sufficient knowledge of the customer, inter alia, to manage the risk of money laundering or terrorist financing that may be associated with the customer relationship (Chapter 3 Section 1 ibid).

4.1.2 Trustly has not defined end users as customers

The investigation has shown that when end users choose to make a payment through Trustly, they instruct the company to execute the transaction and when they do this, they approve the company's general terms and conditions. The

general terms and conditions state that it is Trustly, and not the end user's bank, that provides the service to the end user.

Trustly's business plan and its description of the way its products work show that the company's pay-in service constitutes money remittance that is initiated by a payment initiation. When a payment is made through Trustly, funds are transferred from the payer's account to one of the company's client accounts. The funds are then transferred by the company to the payee's account.

As described in section 1.1, Trustly has referred to the natural persons who use the company's pay-in and pay-out service as 'end users' and the persons who use the company's direct debit service as 'direct debit customers'. During the investigation period, Trustly was of the opinion that end users did not constitute customers as defined in the Money Laundering Act. According to the view expressed by the company at the time, its private customers only comprised the private individuals that used the company's direct debit service, and the corporate customers[8] of the legal entities that used Trustly's services to receive payments from private individuals. If a private individual used both Trustly's direct debit service and any of the company's other products or services, only the direct debit service was used within the customer relationship with the company, in line with the view previously expressed by the company.

Trustly has now changed its view on this. In its statement to Finansinspektionen, Trustly subsequently explained that the company now states that a customer relationship occurs with private individuals who use the company's pay-in service and/or direct debit product and that the company has also identified when a business relationship occurs with an end user. The company has presented an action plan as well that aims to rectify the deficiencies caused by the fact that Trustly has not treated end users as customers.

4.1.3 Observations regarding end users in the sample

Each of the 28 end users that were in Finansinspektionen's sample executed at least 143 transactions to or from gambling companies through Trustly during the eight months covered by the investigation. Several of them have executed as many as over 1,000 such transactions during the period. The combined transactions amounted to considerable sums of money, averaging at more than SEK 8.1 million per person. None of the end users in the sample transferred less than SEK 440,000 to or from gambling companies during the period.

Trustly's end users who generally executed transactions to or from gambling companies during the investigation period (i.e. also covering end users that were not in Finansinspektionen's sample) executed an average of 98 such transactions per person.

[8] Also referred to as 'retailers' by the company.

4.1.4 Risks identified by Trustly regarding end users and the company's measures to prevent these risks

The gambling industry is the business area that accounts for more than half of the combined value of all transactions handled by Trustly. In its general risk assessment the company states that it has assessed the gambling industry as presenting a high risk of money laundering and terrorist financing. The general risk assessment also shows that a significant proportion of all reports of suspicious activities and transactions that Trustly has sent to the Financial Intelligence Unit are related to the gambling industry and that all of these reports have been about end users that Trustly itself did not consider to be customers of the company. It also shows that one of Trustly's main risk scenarios for money laundering is of end users using the company's pay-in and pay-out services to launder money through gambling companies and that the company has assessed that the pay-in and pay-out services present a high risk of money laundering and terrorist financing.

In its statement to Finansinspektionen, Trustly has stated that the company will in future treat end users as customers as defined by the Money Laundering Act. The company therefore states that it will comply with the definition of who a customer is pursuant to Chapter 1 Section 8(4) of the Money Laundering Act.

4.1.5 Finansinspektionen's assessment

The end users are Trustly's customers

The question that Finansinspektionen initially needs to consider is whether Trustly's end users are customers of the company as defined by the Money Laundering Act. If this is the case, the authority has to assess whether Trustly has complied with the money laundering regulatory framework in relation to the end users.

As stated in section 4.1.1, the crucial factor in determining whether someone is a customer or not is if they have entered into, or intend to enter into, a contractual relationship with the payment institution. The investigation has shown that when an end user chooses to make a payment using the company's service, he or she instructs the company to make the payment and at the same time approves the company's general terms and conditions, which stipulate that it is Trustly, and not the end user's bank, that provides the service to the end user. The payment is then executed. It is Finansinspektionen's assessment that this creates a contractual relationship between the end user and Trustly. The end users are therefore covered by the definition of customers pursuant to Chapter 1 Section 8(4) of the Money Laundering Act.

The end users execute transactions

As Finansinspektionen has found that the end users are to be regarded as customers as defined by the Money Laundering Act, the authority then has to

examine whether the other conditions for Trustly to be under an obligation to apply customer due diligence measures in respect of the end users have been met (cf. Government Bill 2016/17:173 p. 230).

Pursuant to Chapter 3 Section 4 second paragraph of the Money Laundering Act, the payment institution must, under certain conditions, apply customer due diligence measures for transactions that exceed certain limits. Transfers of funds referred to in Chapter 3 Section 4 second paragraph (3) are also to be regarded as transactions.

The first question to consider when assessing whether Trustly must apply customer due diligence measures is therefore whether the end users' payments constitute transactions as defined by the Money Laundering Act. The legislative history of the Money Laundering Act states that the term 'transaction' should be interpreted widely, but for the execution of an occasional transaction to require an obliged entity to apply customer due diligence measures, there has to be a transfer of assets to or from the obliged entity (Government Bill 2016/17:173 p. 230).

Pursuant to Chapter 5 Section 8(1) of the Payment Services Act, a supplier may not hold at any time the payer's funds in connection with the provision of the payment initiation services. This means that there is no transfer of assets to the payment institution during the provision of the payment initiation services. However, the legislative history of the provision states that a provider of payment initiation services may also be authorised to provide other payment services for which it may be necessary to hold the payer's funds (Government Bill 2017/18:77 p. 155).

As well as being authorised to provide payment initiation services, Trustly has, inter alia, the authorisation to provide money remittances. The company has described its service as a combination of payment initiation and a money remittance.

When Trustly performs the service, the funds are transferred from the end user's bank account to Trustly's client account or alternatively from Trustly's client account to the end user's bank account. This means that Trustly receives funds from the payer, and therefore holds its funds. This would not have been permitted at all if the company had only been authorised to provide payment initiation services. Consequently, and in light of the way that Trustly's service has been designed, Finansinspektionen's assessment is that the company's service involves the execution of occasional transactions, as there is a transfer of assets to and from the end user when this service is used.

The requirements for customer due diligence measures for occasional transactions pursuant to the Money Laundering Act therefore apply.

Trustly's pay-in and pay-out services are money remittance services

Pursuant to Chapter 3 Section 4 second paragraph (3), customer due diligence measures must be applied if the transaction exceeds an amount corresponding to EUR 1,000, if it involves a transfer of funds as stated in Article 3(9) in Regulation (EU) 2015/847.[9] This definition of a transfer of funds covers several kinds of payments and transfers, if they are at least partially carried out by electronic means. Money remittances, as defined in Chapter 1 Section 4 of the Payment Services Act, are covered by this definition. Finansinspektionen must consider whether Trustly's pay-in and pay-out services are money remittance services.

According to the definition in the Payment Services Act, money remittance is a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, or where such funds are received on behalf of and made available to the payee.

Trustly's payment service involves the company receiving funds from a payer (the end user), without a payment account being created in its name or the name of the payee, for the sole purpose of transferring a corresponding amount to a payee (e.g. a gambling company) or another payment service provider acting on behalf of the payee. This payment service works in a similar way but with a reverse payment flow. Finansinspektionen therefore finds that Trustly's pay-in and pay-out services constitute money remittances. Consequently, the company is obliged to apply customer due diligence measures pursuant to Chapter 3 Section 4 second paragraph (3) of the Money Laundering Act.

All end users in the sample have established a business relationship with Trustly

The requirement for a payment institution to apply customer due diligence measures pursuant to Chapter 3 Section 4 first paragraph of the Money Laundering Act also applies when establishing a business relationship. In this instance this requirement applies without any limits.

The definition of a business relationship in Chapter 1 Section 8(1) of the Money Laundering Act states that a commercial relationship is expected to have a permanence in order to be regarded as a business relationship. The legislative history for the Money Laundering Act also states that a business relationship may arise between a person and an obliged entity as a result of the parties' actual, implicit, actions (Government Bill 2016/17:173 p. 189). The business relationship therefore does not have to arise the first time that the parties have contact with each other. This is something that Finansinspektionen has previously expressed in a supervision report on its experiences from the

[9] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006.

supervision of measures to combat money laundering.[10] In this report FI states that it is of the opinion that a business relationship is normally established when transactions are conducted by the same person and with a frequency of 12 times over a period of 12 months. This report also states that products and services that present a high risk may need to have a narrower definition of the term 'business relationship'. If, during an obliged entity's first contact with the customer, it is not clear to the obliged entity whether the relationship is expected to have sufficient permanence, the obliged entity must continuously assess whether a relationship arises through the parties' implicit actions.

During the investigation period, each end user in Finansinspektionen's sample executed at least 143, and in some cases more than 1,000, transactions to or from gambling companies through Trustly. All of the business relationships between Trustly and the end users in the sample must have been regarded as having the kind of permanence that is required for a business relationship to be considered to be established pursuant to Chapter 1 Section 8(1) of the Money Laundering Act. It is possible that the business relationships had been established before the investigation period, but Finansinspektionen does not have the data to be able to make such an assessment. However, the number of transactions that each end user executed during the investigation period clearly shows that the business relationships were at any rate definitely established during the investigation period.

Trustly has violated its obligations under the Money Laundering Act with regard to the end users

Trustly has violated the Money Laundering Act by not treating the end users as customers as shown above. One direct consequence of Trustly not treating end users as customers is that the company has not complied in a number of ways with specific obligations it has under the money laundering regulatory framework.

General risk assessment

In its general risk assessment, Trustly has indeed stated that one of the main risk scenarios for its operations is that end users use the company's products and services to launder money. However, Trustly has not considered these end users to be *customers* in its general risk assessment. Trustly has therefore not assessed the risk that end users may present as customers of the company, has not assessed the risks of the distribution channels used for the company's products and services that are available to end users, and has not assessed the geographical risks that may be associated with end users. Trustly has also not designed its general risk assessment based on the risks that have been identified in its operations. Its general risk assessment therefore contains the kinds of deficiencies that mean that it has not been able to be used as an acceptable basis

[10] *Tillsynsrapport nummer 1, Erfarenheter från penningtvättstillsynen 2016–2017*. An English translation is available at www.fi.se.

for the company's procedures, guidelines and other measures against money laundering and terrorist financing. Consequently, Trustly has not complied with the provisions in Chapter 2 Sections 1 and 2 of the Money Laundering Act.

Risk classification

As the end users have not been treated as customers of Trustly, none of the end users in the sample had been assigned a risk class. Trustly has therefore not assigned risk classes to the end users in the way required by Chapter 2 Section 3 of the Money Laundering Act.

Procedures and guidelines

Chapter 2 Section 8 first paragraph of the Money Laundering Act states that a payment institution must have documented procedures and guidelines in place for, inter alia, the institution's customer due diligence measures. According to the third section of this paragraph, the scope and content of these procedures and guidelines must be determined based on the institution's size, nature and the risks of money laundering and terrorist financing that have been identified in the general risk assessment.

As Trustly has not treated end users as customers, the company does not have any procedures or guidelines in place for customer due diligence for end users. Although the company has assessed that the end users' transactions to and from the gambling industry present one of the main risks to the company, Trustly has not established procedures and guidelines for customer due diligence for end users. As stated above, Finansinspektionen's assessment is that Trustly executes the kinds of occasional transactions that are referred to in Chapter 3 Section 4 second paragraph of the Money Laundering Act. The company has therefore been under an obligation to establish procedures and guidelines for customer due diligence for such transactions, which it has not done. Finansinspektionen finds that Trustly has therefore not complied with the requirements for procedures and guidelines in Chapter 2 Section 8 of the Money Laundering Act.

Customer due diligence

Chapter 3 of the Money Laundering Act requires obliged entities to have knowledge of their customers and to apply customer due diligence measures. Trustly has not applied any customer due diligence measures for any of the 28 end users in Finansinspektionen's sample. Finansinspektionen's position in this section is that Trustly has been under an obligation to apply such measures. By not doing so, the company has violated its obligations pursuant to the following provisions in Chapter 3 of the Money Laundering Act.

In relation to the end users in the sample, Trustly has not:

- had sufficient knowledge of the customers to manage the risk of money laundering or terrorist financing and to monitor and assess the customers' activities and transactions (Section 1);
- applied customer due diligence measures when establishing business relationships or executing transactions (Section 4);
- identified the customers and checked their identities before the business relationship was established or the transactions were executed (Sections 7 and 9);
- assessed whether the customers are persons in a politically exposed position (PEP customers), or family members or close associates of such a person (RCA customers) (Section 10);
- checked whether the customers are established in a high-risk third country (Section 11);
- obtained information about the purpose and nature of the business relationship (Section 12);
- continually and when necessary followed up on continuous business relationships (Section 13);
- carried out checks and assessments to the extent that is required based on the customer's risk profile and other conditions (Section 14); or
- carried out much more extensive checks and assessments in cases where the risk of money laundering or terrorist financing that may be associated with the customer relationship has been assessed as being high (Section 16).

Monitoring

Chapter 4 of the Money Laundering Act contains provisions on the obliged entity's obligations with respect to monitoring and reporting. Although Trustly has not treated the end users as customers, it has monitored their transactions to some extent. Issues relating to deficiencies in its monitoring are presented in greater detail in section 4.6.

4.2 Inadequate general risk assessment

4.2.1 Regulation

Chapter 2 Section 1 first paragraph of the Money Laundering Act states that a payment institution must assess the ways in which the products and services it provides in its operations may be used for money laundering or terrorist financing and the likelihood of this risk occurring (general risk assessment). The legislative history of the Money Laundering Act states that when a payment institution carries out its general risk assessment, it must answer the question as to whether and how these products and services can be used, for example, to conceal any links between criminally obtained property and crimes or criminal activities (Government Bill. 2016/17:173 p. 510).

The second section of this paragraph states that a specific factor that the payment institution must take into consideration when carrying out its general risk

assessment is whether there are any geographical risk factors. Geographical risk factors are those that relate to the conditions in the countries where products and services are provided or where the payment institution's customers are based (Government Bill 2016/17:173 p. 510).

Chapter 2 Section 1 third paragraph of the Money Laundering Regulations states that a payment institution must update its general risk assessment before it offers new or significantly changed products or services, enters new markets or makes other changes affecting its operations.

4.2.2 Observations

Trustly provides a service called *Pay N Play*. Trustly has described this service as one of the company's core products. It has been specifically developed for the gambling industry and is described by the company as a service that enables fast and easy transfers to gambling companies. The service is a combination of three of the company's existing products: pay-in service, pay-out service and information services. These three products are each included separately in the general risk assessment. However, in the version of the general risk assessment that was used during the investigation period, Trustly did not assess whether the risk for each product had been affected by this specific combination or what risk Pay N Play as such presents. The company has therefore not assessed whether the risk for the products included in Pay N Play is affected by the fact that they are combined in Pay N Play. As Trustly has not carried out a risk assessment of Pay N Play, the company has not updated its general risk assessment before offering new or substantially changed products and services.

The general risk assessment shows that Trustly has made an assumption that all direct debit customers only have a geographical exposure to Sweden. For a direct debit customer who is not a PEP customer or RCA customer, the company has not collected any data about the customer's geographical exposure, such as address, citizenship or tax residence.

Trustly has informed Finansinspektionen that the company has now carried out a review of its direct debit customers' geographical exposure. As a result of this review, business relationships with several hundred direct debit customers were terminated because they were established in a high-risk third country, and with more than one thousand direct debit customers because the company could not rule out that they were established in one of these countries.

4.2.3 Finansinspektionen's assessment

Trustly has admitted that the company has not carried out a risk assessment of its Pay N Play product and therefore not the combination of products included in Pay N Play either. Finansinspektionen finds it remarkable that the company has not carried out such a risk assessment despite the fact that the company has stated that Pay N Play constitutes one of the company's core products and that the product has been specifically developed for a high-risk industry.

Finansinspektionen therefore finds that Trustly has not complied with the requirements in Chapter 2 Section 1 first paragraph of the Money Laundering Act that states that the general risk assessment must include an assessment of the way that the products and services provided in the operations may be used for money laundering or terrorist financing and the extent of this risk. Trustly has also not updated its general risk assessment before the company has offered new or significantly changed products and services, and has therefore not fulfilled its obligations pursuant to Chapter 2 Section 1 third paragraph of the Money Laundering Regulations.

It is not disputed that Trustly has assumed in its general risk assessment that all direct debit customers have only a geographical exposure to Sweden. Finansinspektionen's assessment is that this kind of assumption does not comply with the requirements for the kind of assessment of geographical risks that is referred to in Chapter 2 Section 1 second paragraph of the Money Laundering Act. By omitting the geographical risk that may be associated with direct debit customers, Trustly has not taken into consideration all the geographical risk factors in its operations. This was proven when Trustly's assumption was shown to be completely wrong, when a subsequent review identified that several hundred customers had an exposure to high-risk third countries and that this kind of exposure could not be ruled out for more than one thousand customers. Trustly has therefore not complied with Chapter 2 Section 1 second paragraph of the Money Laundering Act in this respect.

4.3 Inadequate risk classification of customers

4.3.1 Regulation

Pursuant to Chapter 2 Section 3 first paragraph of the Money Laundering Act, a payment institution must assess the risk of money laundering or terrorist financing that may be associated with a customer relationship. This is referred to as the customer's risk profile. This risk profile must be determined based on the general risk assessment and the obliged entity's knowledge of the customer. The third paragraph of Section 3 states that the customer's risk profile must be followed up during continuous business relationships and changed when there is reason to do so.

4.3.2 Observations

The company's procedures and guidelines for its risk classification of customers state that the company must divide its customers into five different risk classes: low, normal, high, very high and unacceptable risk.

Looking at the customer due diligence documentation and other material submitted by Trustly to Finansinspektionen for the 22 direct debit customers in the authority's sample, it is not possible to ascertain whether any of the direct

debit customers have been assigned a risk class, when they were assigned a risk class or which risk class they have been assigned.

Trustly's general risk assessment states that a customer that the company has reported to the Financial Intelligence Unit should be considered to be a customer that presents a very high risk. A total of 12 of the 22 direct debit customers in the sample have been reported to the Financial Intelligence Unit for suspicious activities or transactions linked to gambling companies.

Trustly has stated that when a customer has been reported to the Financial Intelligence Unit, a risk classification must be performed again in accordance with the company's procedures. However, Finansinspektionen has noted that neither the company's procedures for reporting customers to the Financial Intelligence Unit nor the company's procedures for the risk classification of customers state how or when a risk classification must be performed for a customer who has been reported to the Financial Intelligence Unit. Finansinspektionen has also noted that Trustly has not carried out any evaluations or made any changes to the customer's risk class as a result of any of the direct debit customers being reported to the Financial Intelligence Unit.

Trustly has not contested Finansinspektionen's observations.

4.3.3 Finansinspektionen's assessment

The main purpose of the risk-based approach is for obliged entities to be able to adapt their measures to prevent money laundering and terrorist financing from the risks in their operations. Using its general risk assessment and the risk-based procedures, the obliged entity has created a basis for assessing and managing the risks of money laundering and terrorist financing that are specific to its operations. However, the risks in its operations are not static, but vary depending on circumstances relating to the specific customer, the products and services that the customer uses and the way the customer uses these products and services. This means that in principle every customer, following an overall assessment, can be assigned its own risk class and that the measures to prevent the risks can be adapted individually for each customer (Government Bill 2016/17:173 p. 259).

The assessment of the customer's risk profile is referred to as 'risk classification', which means that a customer is assigned a risk class. The customer's risk class must be followed up during continuous business relationships and changed when there is reason to do so. If an obliged entity is to apply risk-based customer due diligence measures and transaction monitoring, it must make an assessment of the risk that the customer presents and this has to be documented and easily accessible for the company's employees. This assessment must be based on the company's general risk assessment and the knowledge the company has of the individual customer.

The customer due diligence documentation submitted to Finansinspektionen does not show that any of the 22 direct debit customers in Finansinspektionen's sample have been assigned an individual risk class. Finansinspektionen's assessment is therefore that Trustly has not fulfilled its obligation pursuant to Chapter 2 Section 3 first paragraph of the Money Laundering Act to assess the risk of money laundering or terrorist financing that may be associated with these customer relationships. Trustly has not contested this assessment.

In its general risk assessment, Trustly has assessed that if a customer is reported to the Financial Intelligence Unit, the customer presents a very high risk of money laundering and terrorist financing. A total of 12 of the direct debit customers in the sample have been reported to the Financial Intelligence Unit. Despite this, Trustly has not carried out any follow-up of these customers' risk profile as a result of them being reported to the Financial Intelligence Unit.

Finansinspektionen's assessment, which is line with what the company states in its general risk assessment, is that the fact that a customer is reported to the Financial Intelligence Unit constitutes a high risk factor. This kind of report must, of course, be taken seriously and result in the customer's risk class being evaluated and, if necessary, adjusted. Finansinspektionen therefore finds that Trustly has not determined the customer's risk profile based on the general assessment and the company's knowledge of the customer for any of the 12 direct debit customers in the sample that have been reported to the Financial Intelligence Unit. Trustly has also not followed up the customer's risk profile during continuous business relationships nor changed it if there has been reason to do so. Trustly has therefore not fulfilled its obligations pursuant to Chapter 2 Section 3 first and third paragraphs of the Money Laundering Act.

4.4 Inadequate procedures and guidelines for customer due diligence

4.4.1 Regulation

Pursuant to Chapter 2 Section 8 of the Money Laundering Act, an obliged entity must have documented procedures and guidelines for, inter alia, its customer due diligence measures.

4.4.2 Observations

None of the versions of the company's procedures and guidelines for customer due diligence measures that Finansinspektionen received describes how or when the company must check whether a direct debit customer is established in a country outside the European Economic Area (EEA) that the European Commission (Commission) has identified as a high-risk third country.

Trustly's general procedure for customer due diligence measures states that the company must obtain data on the purpose and nature of the business relationship. Trustly has also adopted special procedures for obtaining information about the

purpose and nature of the business relationship for corporate customers. There are no corresponding procedures for direct debit customers.

Trustly's procedure for the continuous follow-up of business relationships states that the purpose and background of this procedure are based on the provision that is set out in Chapter 3 Section 13 of the Money Laundering Act, which states, inter alia, that an obliged entity must continuously and, if necessary, follow up on continuous business relationships. The procedure does not state how and when the company must continuously follow up direct debit customers.

Trustly has not contested Finansinspektionen's observations.

4.4.3 Finansinspektionen's assessment

Procedures and guidelines for customer due diligence constitute a basic requirement for the company to be able to apply appropriate, consistent and risk-based customer due diligence measures. The obliged entity's procedures and guidelines are very important for the application of the risk-based approach. In practice, the internal procedures largely replace such detailed provisions in acts or regulations that provide clear and detailed codes of practice (Government Bill 2016/17:173 p. 212).

In several respects, Trustly has not had any procedures and guidelines for customer due diligence measures for its direct debit customers. Finansinspektionen therefore finds that Trustly has not complied with the provisions in Chapter 2 Section 8 of the Money Laundering Act, which states that an obliged entity must have documented procedures and guidelines for, inter alia, its customer due diligence measures.

4.5 Inadequate customer due diligence measures

As stated above, Finansinspektionen has examined the customer files for a total of 50 private individuals, divided into 22 direct debit customers and 28 end users, to assess the customer due diligence measures. The sample includes the direct debit customers and end users who, during the investigation period, transferred the largest combined value to gambling companies and those that the company has reported most often to the Financial Intelligence Unit for suspicious transactions or activities linked to gambling companies during the investigation period.

Finansinspektionen has also examined the customer due diligence measures that the company has applied for nine gambling companies.

In section 4.1.5, Finansinspektionen has presented its assessment of the deficiencies that the authority has observed in Trustly's customer due diligence measures in relation to end users. In this section, Finansinspektionen presents its observations and assessments in relation to direct debit customers and gambling companies.

During the eight months covered by the investigation, all of the direct debit customers in the sample executed at least 44 transactions to and from gambling companies through Trustly. The combined transactions amounted to considerable sums of money, averaging at more than SEK 4.7 million per person. None of the direct debit customers in the sample have transferred less than SEK 320,000 to or from gambling companies during the period.

4.5.1 Inadequate checks of establishment in high-risk third countries

Regulation

Chapter 3 Section 11 of the Money Laundering Act states that a payment institution must check whether a customer is established in a country outside the EEA that has been identified by the Commission as a high-risk third country. If the customer is established in one of these countries, the payment institution must apply enhanced customer due diligence measures for business relationships or occasional transactions pursuant to Section 17 of Chapter 3.

Observations

The customer files for the 22 direct debit customers do not show that Trustly checked whether any of the customers were established in a country outside the EEA that has been identified by the Commission as a high-risk third country.

Finansinspektionen's assessment

Trustly has not contested Finansinspektionen's observations, but stated that the company, at the end of 2020, checked the geographical establishment of direct debit customers. Through this it identified several hundred direct debit customers that were established in a high-risk third country and more than one thousand direct debit customers for which the company could not rule out such an establishment. Consequently, Trustly terminated its business relationships with all of these direct debit customers. These deficiencies have now been rectified.

It is therefore not disputed that Trustly has not checked whether any of the direct debit customers in Finansinspektionen's sample were established in any of the countries outside the EEA that have been identified by the Commission as a high-risk third country. The obligation to check this is absolute. Finansinspektionen therefore finds that Trustly has not fulfilled its obligation pursuant to Chapter 3 Section 11 of the Money Laundering Act in relation to the direct debit customers in the sample.

Finansinspektionen would like to stress that the importance of a payment institution complying with the requirement to check establishments in a high-risk third country is evident, as otherwise the institution risks not taking the enhanced customer due diligence measures that are required for business relationships or

occasional transactions when customers are established in such a country pursuant to Chapter 3 Section 17.

4.5.2 Inadequate information about the purpose and nature of the business relationship

Regulation

Chapter 3 Section 12 of the Money Laundering Act states that a payment institution must obtain information about the purpose and nature of the business relationship.

Observations

In terms of Trustly's direct debit customers, none of the customer due diligence files that Finansinspektionen received contained any information about the purpose or nature of the business relationship, neither about the transactions or activities that take place within the direct debit product nor about transactions through any of the company's other products or services that the direct debit customers have used.

In terms of the nine corporate customers in Finansinspektionen's sample, Trustly has assessed that these customers present a high risk of money laundering and terrorist financing as they are gambling companies. For these corporate customers, the company describes the nature of the business relationship with either an amount or an interval for the value of an average incoming payment. However, in the customer files for these corporate customers, there is an input field for the average amount for outgoing payments, a maximum amount for incoming payments and a maximum amount for outgoing payments; this data was missing in all of the customer files that were examined.

For the corporate customers, Trustly describes the nature of the business relationship using the customer category to which the corporate customer belongs and lists the products and services provided by the customer. For all corporate customers in the sample, the customer category is described as 'gambling' and the description of the customer's products includes words such as 'online casino', 'poker', 'online gambling' and 'sports betting'.

The investigation has revealed that there have been significant differences between the corporate customers in the sample in terms of both the number of transactions and the combined value of the transactions that have been executed.

Trustly has not contested Finansinspektionen's observations, but it has stated that the significant variations in the nature of the business relationships for the gambling companies are not evident in the customer category, but are captured by the company obtaining an average amount and a maximum amount for outgoing payments and incoming payments, as well as the average payment frequency. Furthermore, the company states that the Money Laundering Act does

not set any requirements as to the scope or number of words that must be used when describing the nature of the business relationship. Trustly believes that the company's description is well-balanced and covers the customer categories and products and services that are relevant for determining how the gambling company has intended the service or product to work. Trustly has further stated that it assesses that the measures it has applied mean that it complies with the requirements for obtaining information about the nature of the business relationship pursuant to Chapter 3 Section 12 of the Money Laundering Act in relation to the gambling companies.

Finansinspektionen's assessment

The legislative history of the Money Laundering Act states that there are two main purposes behind the requirement to obtain information about the purpose and nature of the business relationship (Government Bill 2016/17:173 p. 247). One purpose is to provide the payment institution with a basis for assessing the risk of money laundering or terrorist financing that may be associated with the customer in question. The second purpose is to provide the payment institution with a basis for being able to assess the way the customer is expected to act within the framework of the business relationship. The assessment should primarily apply to the activities and transactions that the customer can be expected to take and execute. This kind of assessment is important to ensure that the payment institution can detect any deviations from the customer's expected behaviour.

Finansinspektionen's investigation shows that there have been apparent deficiencies in Trustly's work to obtain information about the purpose and nature of the business relationships with direct debit customers, and information about the nature of business relationships with gambling companies.

As stated above, none of the customer due diligence files for direct debit customers that the authority received contained any data about the purpose or nature of the business relationship. Finansinspektionen's assessment is therefore that as far as the direct debit customers in the authority's sample are concerned, Trustly has completely failed to obtain the information that is required and that Trustly has thereby violated its obligation pursuant to Chapter 3 Section 12 of the Money Laundering Act. This is particularly serious as Trustly has assessed the pay-in and pay-out services as presenting a high risk of money laundering, so it is particularly important for the company to obtain information about the purpose and nature.

In terms of the gambling companies in the sample that have been classified by the company as high risk, Finansinspektionen notes that the data on the nature of the business relationship has been insufficient in every case. Trustly has indeed had some data about the customer category and the customer's products. However, there has been a lack of information in the input fields that relate to the average amount for outgoing payments, the maximum amount for incoming payments and the maximum amount for outgoing payments. As the company

itself has stated, this data was needed to be able to make a correct assessment of the nature of the business relationship. Finansinspektionen's assessment is that on the whole it has not been possible to determine the way the individual customer is expected to use the company's products or services and act within the business relationship from the information that appears in the customer due diligence files. Finansinspektionen therefore finds that as far as the gambling companies in the sample are concerned, the company has not had sufficient data about the nature of the business relationship to be able to assess the way the individual customer is expected to act within the framework of the business relationship. It is Finansinspektionen's opinion that this information is particularly important as all gambling companies in the sample have been assessed as presenting a high risk and there are clear differences between the activities and transactions of these gambling companies.

Consequently, as far as the gambling companies in the sample are concerned, Trustly has not complied with the requirements in Chapter 3 Section 12 of the Money Laundering Act that stipulate that the company must obtain information about the nature of the business relationship.

4.5.3 Inadequate continuous follow-up of direct debit customers

Regulation

Pursuant to Chapter 3 Section 13 of the Money Laundering Act, a payment institution must continually and when necessary follow up continuous business relationships in order to ensure that its knowledge of the customer is up-to-date and sufficient to manage the assessed risk of money laundering or terrorist financing.

Observations

In the material that Finansinspektionen received as part of its investigation, there is no documentation for any of the direct debit customers in the sample to show that Trustly has carried out any continual follow-up of the business relationship since it was established.

Trustly has not contested Finansinspektionen's observations, but stated that the company has carried out some continual follow-up of the business relationships in the form of regular checks as to whether the customer is a PEP customer or an RCA customer.

Finansinspektionen's assessment

Continual follow-up of the business relationship refers to regular checks to ensure that the knowledge of the customer is up-to-date, correct and sufficient based on the customer's risk profile. As with the other customer due diligence measures, this follow-up is based on the risk that may be associated with the customer relationship. Consequently, the continual follow-up should be more

extensive and be carried out more frequently, the greater the risk associated with the customer relationship is (Government Bill 2016/17:173 p. 527).

The legislative history of the Money Laundering Act states that the continual follow-up of the business relationship has two different purposes (Government Bill 2016/17:173 p. 249). The first purpose is to ensure that the knowledge of the customer is up-to-date, correct and sufficient based on the risk that may be associated with the customer. If the customer's behaviour or use of products and services changes, the knowledge of the customer must normally be updated, supplemented or expanded to respond to the changed risk profile that has resulted from the customer's new behaviour. Knowledge of the way the customer normally conducts their operations and uses the obliged entity's products and services must form the basis of the second purpose; which is to detect any deviating activities and transactions. This is to prevent the customer from using the payment institution for money laundering or terrorist financing.

Finansinspektionen notes that Trustly has not applied any measures to continually follow up the business relationship with its direct debit customers in the sample, other than to check whether the customer is a PEP or RCA customer. The company has therefore not checked whether its current customer knowledge is up-to-date and sufficient in the manner required by the Money Laundering Act. The follow-up measures that Trustly has stated that the company has carried out have not been clearly documented in the company's customer due diligence files. In addition, these measures alone could scarcely form the basis for Trustly's work to detect deviating activities and transactions. Finansinspektionen therefore finds that Trustly has not followed up its business relationships with its direct debit customers continually and when necessary, and that the company has therefore not complied with the requirements in Chapter 3 Section 13 of the Money Laundering Act.

4.5.4 Inadequate enhanced measures for customers assessed as being high risk

Regulation

Chapter 3 Section 16 of the Money Laundering Act states that a payment institution must perform much more extensive checks, assessments and investigations as part of its customer due diligence measures if the risk of money laundering or terrorist financing that may be associated with the customer relationship is assessed as being high.

Observations

As stated in section 4.3 above, Trustly considers that customers that have been reported to the Financial Intelligence Unit present a very high risk. The company's procedures and guidelines for customer due diligence state that the company must apply enhanced customer due diligence measures for the customers that have been assigned this risk class. A total of 12 of the 22 direct

debit customers in Finansinspektionen's sample have been reported to the Financial Intelligence Unit for suspicious activities or transactions linked to gambling companies, and several of these customers have been reported more than once during the eight months covered by the investigation. The material that Finansinspektionen received as part of its investigation shows that the company has not applied any enhanced customer due diligence measures for any of the customers that have been reported to the Financial Intelligence Unit.

The company's general risk assessment states that Trustly has assessed that gambling companies present a high risk of money laundering and terrorist financing. The company therefore has a specially designed customer due diligence form for these customers. Trustly's customer due diligence files for gambling companies contain a section with information about the customer's risk class and the customer's measures to prevent money laundering, as well as something the company refers to as 'regulatory considerations'. This section contains a field where Trustly must enter any information about red flags that have been identified with respect to the customer.

Trustly has identified at least one red flag for all of the gambling companies in the sample. Trustly has identified as many as ten red flags for one of the gambling companies. The red flags that have been identified for the gambling companies have, for example, been that the gambling company has been repeatedly involved in reports of suspicion to the Financial Intelligence Unit, that the gambling company has been the subject of an intervention by relevant authorities or that the gambling company has been uncooperative in its contact with Trustly.

The customer due diligence files reveal that the red flags that have been identified have not resulted in any assessment as to whether there is any need for additional customer due diligence measures or whether these red flags have had an impact on Trustly's assessment of the risk associated with the customer relationship. In most cases, Trustly has not applied any measures as a result of the red flags that have been identified, apart from noting the information that led to the red flag in its customer due diligence system.

For one of the gambling companies, Trustly produced a special report on this gambling company and its ability to prevent money laundering, as a result of the red flags that had been identified for this customer. The report states that Trustly had identified a number of risk factors that meant that the customer relationship with the gambling company was associated with a particularly high risk, as the gambling company's measures to prevent money laundering and terrorist financing were insufficient. This report also contains various measures that Trustly has applied in relation to this gambling company.

According to Trustly's general risk assessment, as well as its procedures and guidelines for customer due diligence, the company must check the gambling companies' measures to prevent money laundering in order to reduce the risk associated with the customer relationship. The customer due diligence

information that Trustly has submitted to Finansinspektionen about its corporate customers states that the company has not obtained any underlying documentation about its customers' measures to prevent money laundering for two of the nine gambling companies. For the other seven customers, it appears that the procedures and guidelines obtained by Trustly are at least two years and in some cases up to five years old.

Trustly's position

Trustly has not contested Finansinspektionen's observations, but has stated that the company does not believe that the risk has to be increased and enhanced measures applied pursuant to Chapter 3 Section 16 of the Money Laundering Act as a result of each red flag that is identified. According to the company, the red flags are defined in such a way that not every single red flag is assessed as being serious enough or a strong indication of an elevated risk to automatically prompt an adjustment of the customer's risk profile. The company carries out an assessment of each red flag that has been identified in order to determine whether it means that the risk class has to be adjusted and enhanced customer diligence measures applied.

As for the gambling company about which Trustly produced a special report, the company has stated the following. When there were suspicions of deficiencies in the gambling company's ability to prevent money laundering, Trustly contacted the gambling company immediately to ask it to take action and it set requirements for the gambling company to make improvements. Trustly also introduced its own restrictions for the gambling company's transactions through the company. Trustly made it clear to the gambling company that it would be excluded from Trustly's pay-out service if the problem was not rectified within a specific period of time. The gambling company went on to make improvements.

In terms of Trustly's measures to check the gambling companies' measures to prevent money laundering and terrorist financing, Trustly has objected, stating that it is not always necessary to obtain underlying documentation; only if this is necessary for the company's assessment of its customer knowledge.

Finansinspektionen's assessment

<u>Inadequate handling of red flags</u>

The legislative history of the Money Laundering Act states that enhanced customer due diligence measures mean that the checks, assessments and investigations that have to be carried out pursuant to the customer due diligence provisions must be more extensive than when there is a normal risk of money laundering or terrorist financing (Government Bill 2016/17:173 p. 264). These measures may include, for example, obtaining additional information about the customer's business operations and its financial situation, as well as data about where the customer's financial resources come from.

Finansinspektionen has noted that Trustly has not applied any enhanced due diligence measures for the direct debit customers that the company has reported to the Financial Intelligence Unit and that, in accordance with the company's general risk assessment, have presented a very high risk of money laundering and terrorist financing. Finansinspektionen has also found that during the eight months covered by the investigation, Trustly reported no less than 12 of the 22 direct debit customers in the sample to the Financial Intelligence Unit, and that several of these customers were reported more than once during the period. Finansinspektionen finds it remarkable that the company has nevertheless not applied any enhanced customer due diligence measures for any of these customers. Finansinspektionen therefore finds that Trustly has not complied with the requirements to apply enhanced customer due diligence measures pursuant to Chapter 3 Section 16 of the Money Laundering Act in respect of the direct debit customers that the company has reported to the Financial Intelligence Unit.

The investigation shows that in most cases Trustly has not applied any other measures as a result of the red flags that the company has identified for the gambling companies, other than noting this information in its customer due diligence system. In light of the nature of the red flags and the fact that Trustly has assessed that the gambling companies present a high risk, Finansinspektionen believes that Trustly should have applied additional measures.

Trustly has objected, stating that a red flag does not always constitute a high-risk factor and that the company has acted in accordance with its procedure. However, Finansinspektionen believes that situations where gambling companies have been linked to reports of suspicion to the Financial Intelligence Unit, have been uncooperative with the company or have been the subject of interventions by other authorities are typically considered to be factors that indicate an elevated risk associated with the customer relationship. Finansinspektionen therefore assesses that the red flags in the sample are of such a nature that there have been clear grounds for the company to apply enhanced customer due diligence measures. Trustly has not applied any such measures or carried out any assessments to see whether there have been any grounds to apply additional measures. The company has also not assessed whether the red flags have had an impact on the risk associated with the customer relationship. Finansinspektionen therefore finds that Trustly has not carried out checks, assessments and investigations that are extensive enough as a result of the red flags that the company has identified.

The fact that Trustly has produced a special report in one case does not change this assessment. Although the report indeed states that the company has applied measures as a result of the red flags that had been identified for the specific customer, it is Finansinspektionen's opinion that the measures applied are not commensurate with the high risk that appears in the report. Finansinspektionen has noted that when Trustly contacted the gambling company, it was uncooperative, it did not want to take the measures requested by Trustly and it did not take the measures within the period of time requested by Trustly. This

means that Finansinspektionen considers the measures applied by Trustly to be inadequate.

Finansinspektionen therefore finds overall that Trustly's handling of red flags has been such that the company has violated the requirement in Chapter 3 Section 16 of the Money Laundering Act with regard to taking enhanced customer due diligence measures.

Inadequate evaluation of the gambling companies' measures to prevent money laundering

As stated earlier, Trustly has assessed that the gambling companies present a high risk of money laundering and terrorist financing. According to Trustly's general risk assessment, as well as its procedures and guidelines for customer due diligence, the company must evaluate the gambling companies' measures to prevent money laundering in order to reduce the risk associated with the customer relationship. The investigation shows that Trustly has nevertheless not obtained nor examined updated versions of the gambling companies' procedures and guidelines for preventing money laundering. Finansinspektionen's assessment is therefore that, in light of the risk that the company has assessed the gambling companies to present, Trustly has scarcely assessed the measures that the gambling companies in the sample have taken to prevent money laundering and terrorist financing. It is the view of Finansinspektionen that the objections in this section that have been raised by Trustly, which has stated that the questions that the company asks in its customer due diligence form for the gambling companies is sufficient, can be dismissed because of the high risk that gambling companies present.

Finansinspektionen therefore finds that Trustly has not complied with the requirements in Chapter 3 Section 16 of the Money Laundering Act in this respect either, with regard to taking enhanced customer due diligence measures.

4.5.5 Maintaining business relationships and executing transactions without sufficient knowledge of direct debit customers

Regulation

Chapter 3 Section 1 of the Money Laundering Act states that an obliged entity may not establish or maintain a business relationship or execute occasional transactions if the obliged entity does not have sufficient knowledge of the customer to enable it to manage the risk of money laundering and terrorist financing that may be associated with the customer relationship and monitor and assess the customer's activities and transactions pursuant to Chapter 4 Sections 1 and 2.

Observations

In sections 4.5.1–4.5.4 above, Finansinspektionen has found that as far as direct debit customers are concerned, Trustly has not fulfilled its obligations in several respects in relation to taking customer due diligence measures as set out in the Money Laundering Act.

As has been shown, all 22 direct debit customers in Finansinspektionen's sample executed a large number of transactions to and from gambling companies during the investigation period. It has also emerged that both the gambling industry and the company's products used in transactions to or from the gambling industry by the company have been assessed as presenting a high risk of money laundering and terrorist financing.

Trustly has not contested Finansinspektionen's observations.

Finansinspektionen's assessment

The legislative history of the Money Laundering Act states that the risk-based approach means that it is not possible to set a general minimum level for the scope of one or more customer due diligence measures and that in some cases the circumstances may be such that the risk of a particular product or service is so low that the obliged entity is not required to apply all the customer due diligence measures set out in Article 13 first paragraph a, b or c of the Anti-Money Laundering Directive (Government Bill 2016/17:173 pp. 253).

Finansinspektionen has noted that the company has not obtained information about the purpose and nature of the business relationship for the transactions and activities that direct debit customers execute, has not checked whether its direct debit customers were established in a high-risk third country or has not carried out any continual follow-up of the knowledge the company has had about these customers. Furthermore, Finansinspektionen has noted that the company has not applied any enhanced customer due diligence measures for the 12 direct debit customers that it reported to the Financial Intelligence Unit for suspicious transactions linked to gambling companies. Finansinspektionen has also noted that during the investigation period all 22 direct debit customers executed a large number of transactions of considerable value to and from gambling companies, and both the gambling industry and the company's products used in transactions to or from the gambling industry by the company were assessed as presenting a high risk of money laundering and terrorist financing.

Finansinspektionen can therefore state that the company has not applied basic customer due diligence measures and in some cases it has not applied enhanced measures for customers that have used high-risk products to transfer funds of considerable value to or from a high-risk industry.

It is Finansinspektionen's opinion that Trustly could scarcely have been able to manage the risk of money laundering or terrorist financing that may be

associated with the customer relationship or monitored the transactions and activities that the company's direct debit customers carry out to or from the gambling industry without taking basic and appropriate customer due diligence measures. Overall, it is therefore Finansinspektionen's opinion that the company has not obtained sufficient knowledge of its direct debit customers in several respects. Despite this, the company has maintained business relationships with them and allowed them to execute a large number of transactions.

Finansinspektionen therefore finds that Trustly has violated the ban in Chapter 3 Section 1 of the Money Laundering Act on establishing or maintaining a business relationship or executing occasional transactions, if the obliged entity does not have sufficient knowledge of the customer to be able to manage the risk of money laundering or terrorist financing.

4.6 Inadequate monitoring of continuous business relationships

4.6.1 Trustly's design of its business relationship monitoring

Regulation

Chapter 4 Section 1 first paragraph of the Money Laundering Act states that a payment institution must monitor continuous business relationships and assess occasional transactions in order to, inter alia, detect any activities and transactions that

- deviate from what the institution has cause to expect given the knowledge it has about the customer; or
- deviate from what the institution has cause to expect based on the knowledge the institution has about its customers, the products and services it provides, the data submitted by the customer, and other circumstances.

The second paragraph of this section states that the focus and scope of the monitoring must be determined by taking into account the risks that have been identified in the general risk assessment, the risk of money laundering and terrorist financing that may be associated with the customer relationship and any other information on the approach to money laundering or terrorist financing.

Observations

Trustly has a transaction monitoring system that automatically generates an alert if a certain criterion is met, for example if the value of a certain type of transaction exceeds a set threshold. The company has specific scenarios for direct debit customers, end users and gambling companies respectively. Although Trustly has not explicitly assessed end users as customers, the company has to some extent monitored the end users' transactions and activities as part of its monitoring. During the investigation, Trustly has stated that the reason for this is that the end users' transactions are part of the transactions of

the company's corporate customers and that the monitoring of these transactions is part of the process to better understand and monitor the gambling companies.

Trustly monitors the end users' transactions for each gambling company separately, and the threshold for one scenario only applies to transactions to or from the individual gambling company. For an alert to be generated, the threshold therefore has to be exceeded through transactions to or from an individual gambling company. However, an alert is not generated in Trustly's transaction monitoring system if an end user executes transactions with several different gambling companies and the transactions combined exceed a specific threshold.

In its monitoring system, Trustly separates the transactions that one individual person executes by using the direct debit service, and the pay-in and pay-out services. Similarly, Trustly is also not able to link all the transactions executed by an end user to one specific person, as the company does not always know the end user's identity. By contrast, the company can always link transactions to one specific bank account. However, an end user may use several bank accounts without Trustly always being able to link these accounts to the same natural person.

As stated earlier, one of the main risk scenarios that Trustly has identified in its general risk assessment is that end users use the company's products and services to launder money through gambling companies. Trustly also states that the company's direct debit product presents a low risk, while the pay-in and pay-out products present a high risk.

Trustly's procedures for monitoring show that the company's monitoring scenarios contain a number of scenarios that have been specifically adapted to the direct debit product, and the pay-in and pay-out services, respectively. It appears that the thresholds for the direct debit service are much lower than the thresholds for the pay-in and pay-out services in terms of transactions to and from gambling companies. During the investigation, Trustly has stated that the differences in thresholds are due to the fact that the company had believed that direct debit customers were customers of the company, while end users (according to the company) were not, so the company needs to examine the transactions executed by the direct debit customers more carefully.

Trustly has not contested Finansinspektionen's observations, but has stated that thresholds in the monitoring of a specific service must be determined not only based on the assessed risk, but also on the basis of what is a normal, non-anomalous, use of the service. The company believes that it has set its thresholds by taking into account the differences in the company's expectations for the end users' payments to gambling companies on the one hand and direct debit customers' payments on the other, as well as any differences in the risks that each type of transaction may be associated with. The company believes that it would not be consistent with the Money Laundering Act to lower the thresholds in its monitoring of transactions for the pay-in service to the thresholds that it

applies for the direct debit product, nor to reverse the thresholds in its monitoring of the direct debit product.

Finansinspektionen's assessment

The Fourth Anti-Money Laundering Directive[11] states that a customer due diligence measure that the obliged entity must apply is the ongoing monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the obliged entity's knowledge of the customer, the operations and risk profile. (Article 13.1 d).

Examples of the type of behaviour that obliged entities have to pay attention to are set out in Article 18(2) of this directive. It states that complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose must cause the obliged entity to examine the background and purpose of these transactions and increase the degree and nature of monitoring of the business relationship, in order to determine whether these transactions or activities appear suspicious. The obliged entity must inform the Financial Intelligence Unit and file a report where the obliged entity knows, suspects or has reasonable grounds to suspect that funds are the proceeds of criminal activity or are related to terrorist financing (Article 33(1)(a); cf. also Government Bill 2016/17:173 p. 287).

One of the main reasons for applying customer due diligence measures is for the obliged entity to obtain data to enable it to assess how the customer may be expected to act within the framework of the business relationship. However, the scope of this data will vary depending on the risk that may be associated with the customer relationship. Consequently, there will be individual expectations for specific customers. However, in the majority of cases, it is likely that the obliged entity's assessment of what may be expected of the customer is based on the way that customers in general use the products or services provided by the obliged entity. This should normally also be the case for customers who carry out occasional transactions outside business relationships (Government Bill 2016/17:173 p. 288).

Design of monitoring systems

Finansinspektionen would like to start by stating that the assessment made above in section 4.1.5 and which means that the end users are Trustly's customers shows that Trustly has been under an obligation to monitor the end users during the investigation period. Finansinspektionen also notes that although Trustly did

[11] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.

not consider the end users as customers during the investigation period, it still monitored them and that this, according to the company, was carried out as part of its monitoring of the gambling companies. The company has had specific scenarios for the end users. The alerts generated for these scenarios have been directed at the specific end user and their transactions or activities, and not those of the gambling company.

Section 4.1.5 addresses a number of deficiencies that occurred as a direct consequence of Trustly not treating the end users as customers and therefore has not applied the measures required under the money laundering regulatory framework. However, the situation is different for the monitoring of end users, as Trustly has actually applied certain measures in this area. Finansinspektionen therefore has to examine, inter alia, whether the monitoring carried out by Trustly of the end users complies with the requirements set out in the money laundering regulatory framework.

During the investigation period Trustly has not always had knowledge of all of the transactions and activities that have been carried out by its direct debit customers and end users within the framework of a business relationship, as the company has not always known the identity of the end users who have executed transactions to and from gambling companies. Trustly has also monitored all of the transactions of direct debit customers and end users, based on the transactions executed by the customer with each gambling company individually, and not based on all the transactions that the person has executed through Trustly. As Finansinspektionen has found in sections 4.1 and 4.5, Trustly has also not applied any customer due diligence measures for end users or the transactions executed by direct debit customers. During the investigation it has also emerged that Trustly's monitoring system has not been designed in such a way that it takes into consideration the customer due diligence information that is obtained.

The regulations set requirements for a payment institution to design its monitoring system so that it takes into account the customer due diligence information that is obtained. It is Finansinspektionen's opinion that if a payment institution is to be able to monitor continuous business relationships, the institution must have knowledge of all transactions and activities carried out within the framework of the business relationship and that these must be taken into consideration in the payment institution's ongoing monitoring of continuous business relationships. It is important for a payment institution, such as Trustly, with a high exposure to the gambling industry to be able to detect deviations in transactions to and from several different gambling companies. This is evidenced by the Commission's Supranational Risk Assessment, which states that one common approach to money laundering in the gambling industry involves the use of more than one gambling company.[12] Finansinspektionen further considers that a payment institution cannot detect activities and transactions that deviate from what the payment institution has cause to expect based on the knowledge

[12] Appendix to the EU Supranational Risk Assessment 2019, p. 220.

the institution has about its customers without first having applied customer due diligence measures with respect to them.

Chapter 4 Section 1 first paragraph (1)(2) of the Money Laundering Act stipulates that a payment institution must monitor continuous business relationships and assess occasional transactions in order to detect activities that deviate, inter alia, from what the institution has cause to expect based on the knowledge it has about its customers. Finansinspektionen notes that Trustly has not always had knowledge of all of the transactions and activities carried out within the framework of a business relationship, that Trustly has not monitored the transactions of direct debit customers and end users based on the combined transactions executed by the person through Trustly, and that the company has neither obtained nor taken into consideration customer due diligence information in its ongoing monitoring. It is therefore clear that Trustly has violated its obligations pursuant to Chapter 4 Section 1 first paragraph (1)(2) of the Money Laundering Act with respect to both end users and direct debit customers.

Risk-based monitoring

A payment institution's monitoring must be determined, inter alia, by taking into consideration the risks that have been identified in its general risk assessment.

The legislative history of the Money Laundering Act states that a starting point for a payment institution's monitoring of transactions should be the risk assessment that the institution has carried out (Government Bill 2016/17:173 p. 289). As described in section 3.6, one of the main risk scenarios for money laundering and terrorist financing identified by Trustly in its general risk assessment is that end users use the company's products and services to launder money through gambling companies. Trustly has also assessed that both the gambling industry and the pay-in and pay-out service present a high risk of money laundering and terrorist financing, while the direct debit service presents a low risk. The thresholds set by Trustly in its scenarios for transactions with gambling companies have been much lower for the direct debit product than for the pay-in and pay-out services.

Finansinspektionen states that Trustly, in line with the risk-based approach in the money laundering regulatory framework, needs to adapt its monitoring to the risks identified by the company. During the investigation period, Trustly has not always been able to see all of the transactions that a customer executes to and from gambling companies. Neither has Trustly monitored transactions to and from gambling companies collectively, but only for each gambling company individually. Furthermore, Trustly has not determined the thresholds in its monitoring based on the risk presented by the products as assessed by the company.

Finansinspektionen states that the regulatory framework requires that a payment institution's focus and scope of its monitoring must be determined based on the

risks that have been identified in its general risk assessment. In light of what has been stated above, Finansinspektionen's assessment is therefore that Trustly's monitoring has not been designed on the basis of the company's general risk assessment and that Trustly has therefore not complied with the requirements in Chapter 4 Section 1 second paragraph of the Money Laundering Act.

Trustly has objected, stating that the thresholds for this monitoring cannot be determined solely on the basis of the risk presented by a product or service. However, Finansinspektionen has not made its assessment solely based on the size of the thresholds in question, but finds that overall, based on what has been stated above, Trustly's monitoring of business relationships has not been designed in line with the risk-based approach in the money laundering regulatory framework. The objection raised by Trustly therefore does not change this assessment.

4.6.2 Investigation of alerts in Trustly's monitoring system

Regulation

Pursuant to Chapter 4 Section 2 first paragraph of the Money Laundering Act, if a payment institution detects any deviations or suspicious activities or transactions as a result of its monitoring or in any other way, it must apply enhanced customer due diligence measures and other necessary measures to assess whether there are reasonable grounds to suspect that they constitute money laundering or terrorist financing or that property otherwise derives from criminal activity.

Observations

Finansinspektionen has examined ten alerts that were generated during the investigation period in Trustly's system for monitoring transactions executed by the direct debit customers (two of them) and end users (eight of them) in the sample. Finansinspektionen has also examined the measures that the company has applied as a result of these alerts.

Screenshots from Trustly's transaction monitoring system show that seven alerts were dismissed with the same general comment. This comment also appears in the company's procedures for monitoring transactions as a suggested comment that can be used to dismiss an alert. The comment states that the alert is for an individual who has several bank accounts and accounts with several different gambling companies, but this alert can be dismissed without suspicion. Judging by the screenshots, this comment is the only documented investigative measure that has been applied for these seven alerts.

It also appears that the company has not applied any customer due diligence measures for eight of the customers where alerts were generated because they were end users. At the same time, Finansinspektionen notes that all eight

customers have executed a large number of transactions to and from gambling companies, to a value of at least SEK 6 million per person.

Trustly has not contested Finansinspektionen's observations, but has stated that it believes that enhanced customer due diligence measures do not have to be applied for every alert that is generated, even if the investigative measures applied in the cases examined by Finansinspektionen have not been sufficient in relation to the risks that these situations have been associated with.

Finansinspektionen's assessment

The legislative history of the Money Laundering Act states that deviating transactions must cause the obliged entity to apply customer due diligence measures, which in turn aims to ensure that the obliged entity can assess whether deviations or suspicions of money laundering and terrorist financing can be dismissed or not. If suspicion still remains after customer due diligence measures have been applied, the obliged entity must file a report with the Financial Intelligence Unit.

Finansinspektionen's assessment is that the measures applied for eight of the ten alerts, and which referred to end users and direct debit customers in Finansinspektionen's sample, have not been sufficient bearing in mind the risk that the company has assessed these transactions to present. This is because the company has not applied any more detailed investigative measures, despite not having sufficient knowledge of the customers. The company has therefore not been in a position to make an assessment as to whether the transactions executed by an individual customer have been anomalous or in any way suspicious.

Investigating and reacting to alerts of this kind are crucial if the money laundering regulatory framework is to be effective. Finansinspektionen therefore finds it remarkable that although the transactions that preceded the generated alerts were the ones that the company has identified as being among the company's main risks for money laundering, Trustly has not applied any customer due diligence measures or sufficient investigative measures when investigating the alerts.

Trustly has objected, stating that it would be too broad-based if every alert were to prompt a detailed investigation, including enhanced customer due diligence measures, rather than making an assessment based on the individual alert. However, Finansinspektionen's assessment is based on the fact that the alerts that have been the subject of the current investigation have required enhanced investigative measures and that the measures applied by the company were not sufficient in the cases in question. Consequently, the objection raised by Trustly does not change this assessment.

Finansinspektionen's assessment is therefore that the company has not complied with the requirements in Chapter 4 Section 2 first paragraph of the Money Laundering Act.

4.6.3 Procedures for model risk management in relation to monitoring

Regulation

Pursuant to Chapter 6 Section 1 second paragraph of the Money Laundering Act, if a payment institution uses models for monitoring, it must have procedures for model risk management. These procedures must aim to evaluate and ensure the quality of the models used by the institution.

Chapter 6 Sections 16 and 17 of the Money Laundering Regulations state that the payment institution must carry out a validation of a model before it is used and if there are any significant changes to the model, and that the institution must produce a report on the results of the validation after each validation.

Observations

Trustly's transaction monitoring system is mostly based on automated scenarios with predetermined thresholds that determine when an alert is generated in the system. The investigation has shown that the company has not considered its monitoring system as the kind of model referred to in Chapter 6, section 1 of the Money Laundering Act and that it has not had any procedures for model risk management or validated the model.

Trustly has not contested Finansinspektionen's observations.

Finansinspektionen's assessment

The legislative history of the Money Laundering Act states that models may be used, inter alia, to simplify and systematise the monitoring of transactions (Government Bill 2016/17:173 p. 213). It also states that monitoring models can include, for example, automated monitoring systems that are programmed to warn of or flag transactions that are considered by obliged entities to be associated with high risk or otherwise anomalous (see Government Bill 2016/17:173 p. 547). Finansinspektionen has also communicated this in its Q&As.[13]

During the investigation period, Trustly had an automated monitoring system that used scenarios with predetermined thresholds to detect deviating transactions. This kind of system is a monitoring model as defined in the legislative history of the Money Laundering Act. Trustly has therefore been under an obligation to establish procedures for model risk management, to validate the model and to produce a report on this validation, which the company has not done. Consequently, Trustly has violated its obligations pursuant to Chapter 6 Sections 11 of the Money Laundering Act and Chapter 6 Section 16 and 17 of the Money Laundering Regulations during the investigation period.

[13] Finansinspektionen's Q&As: https://www.fi.se/sv/sok-tillstand/fragor-och-svar/.

5 Considerations for the intervention

5.1 Applicable provisions

The Money Laundering Act and the Money Laundering Regulations are the other kinds of legislative framework that govern the company's operations that are referred to in Chapter 8 Section 8 of the Payment Services Act. Finansinspektionen must therefore apply the following provisions from the Payment Services Act when considering whether to intervene for violations of the Money Laundering Act and the Money Laundering Regulations.

Chapter 8 Section 8 states that Finansinspektionen must intervene, inter alia, if a payment institution violates its obligations stipulated in the act, other parts of the legislative framework that governs the institution's operations, or internal instructions based on the legislative framework that governs the institution's operations.

Finansinspektionen can intervene by ordering the payment institution to implement measures that will rectify deficiencies or by issuing the institution with a remark. If the violation is serious, the authorisation of the payment institution must be revoked, or, a warning issued, if this is judged to be sufficient.

Chapter 8 Section 9 first paragraph states that when determining the intervention, Finansinspektionen must take into consideration the gravity of the violation and its duration. Special consideration must be taken of any damage that has been caused and the degree of responsibility.

The second paragraph in this section states that Finansinspektionen may refrain from intervening pursuant to Section 8 if the breach is negligible or excusable, if the payment institution rectifies the case or if any other authority has taken measures against the institution and these measures are deemed sufficient.

Chapter 8 Section 9a first paragraph states that in addition to what is set out in Section 9, Finansinspektionen must also take into consideration any previous violations by the payment institution as an aggravating circumstance.

The second paragraph of this section states that when looking at mitigating factors, consideration should be taken of whether the institution has cooperated actively to a significant extent to facilitate Finansinspektionen's investigation and whether the institution has quickly ceased with the violation once it has been reported or identified by Finansinspektionen.

Pursuant to Chapter 8 Section 14 Finansinspektionen may combine a remark or warning with an administrative fine.

Chapter 8 Section 15a states that if there has been a violation of the Act on Measures against Money Laundering and Terrorist Financing (2017: 630) or regulations that have been issued pursuant to this act, the administrative fine that can be determined pursuant to Chapter 8 Section 14 must be a minimum of SEK 5,000 and a maximum of the highest of:

1. 10% of the payment institution's turnover for the preceding financial year or, where applicable, the corresponding turnover at group level;
2. twice the profit recorded by the institution as a result of the violation of the rules, if this amount can be determined; or
3. an amount in Swedish krona that is the equivalent of EUR 5 million.

Chapter 8 Section 15a second paragraph states that the fine must not be so high that the institution is subsequently not able to comply with the requirements pursuant to Chapter 3 Section 2 of this act.

When determining the amount of the administrative fine, special consideration, pursuant to Chapter 8 Section 16, should be given to the kind of circumstances that are set out in Section 9 first paragraph, and section 9a, as well as to the payment institution's financial position, and the profit the payment institution realised as a result of the violation, if this can be established.

5.2 Trustly's position

Trustly has stated that the company takes the deficiencies identified by Finansinspektionen very seriously. The company has also stated that it takes the work against money laundering and terrorist financing very seriously and takes a very serious view of the criticism and deficiencies described by Finansinspektionen. Trustly has also stated that the company has allocated, and continues to allocate, substantial resources to rectify the deficiencies. According to the company, these measures include, inter alia, a directive for risk prioritisation by the Board of Directors and a strengthening of the organisation.

The observations and assessments made by Finansinspektionen have prompted the company to produce an action plan that it is continuously working with. The company has presented the measures it has applied and submitted the action plan that the company is following. According to the action plan, the company will implement the measures by the final quarter of 2022. By the time the company replied to Finansinspektionen's verification letter in May 2021, the company had applied several of the measures, while others were ongoing or had been planned. The measures that Trustly stated that the company had applied or was planning to apply include the company now defining that it has a customer relationship with private individuals who use the company's pay-in service or direct debit product, from the first time this service is provided. This means that in the future the company will treat end users as customers as defined in the Money Laundering Act. Trustly has also stated that the company now identifies that its interaction with an end user may constitute a business relationship.

Trustly has firstly requested Finansinspektionen to refrain from intervening. However, if Finansinspektionen were to assess that an intervention is still necessary, it is Trustly's opinion that the authority should take into consideration a number of circumstances that the company believes are mitigating circumstances. The company believes that the deficiencies identified in the investigation are largely attributable to the company not previously defining end users as customers. According to Trustly, the deficiencies relating to end users should be considered to be excusable or at least not reprehensible for two reasons. Firstly, the company has stated that it based its previous position on a careful and prudent assessment that was founded on relevant legal guidance. Secondly, the company has stated that it had reason to believe that Finansinspektionen shared the company's view as Finansinspektionen had decided to close a previous investigation (case FI Ref. 13-4173) without taking any further action. Trustly therefore believes that the deficiencies in relation to end users are due to a behaviour that in view of the special circumstances should be considered less reprehensible than would otherwise be the case, and are therefore also excusable.

Trustly has also requested that when Finansinspektionen makes a decision on whether to intervene, and if so, which kind of intervention it takes, it should consider the measures that the company has taken and intends to take in order to rectify the deficiencies that have been identified, and that the company has acted quickly in its work to rectify these deficiencies. Trustly has also stated that the deficiencies that the company is guilty of have not been intentional nor systematic. Trustly also considers that the violations alleged by Finansinspektionen have not resulted in any actual damage or risk of damage, and that the risk of actual money laundering or terrorist financing in the company's operations has been limited.

5.3 These violations require an intervention

In section 3.6, Finansinspektionen's assessment was that as Trustly's operations target the gambling industry, it has high exposure to an industry that presents a particularly high risk of money laundering and that the company's role in the payment chain puts it in a unique position to identify and prevent money laundering or terrorist financing linked to transactions to and from the gambling industry. Furthermore, the money laundering regulatory framework ultimately aims to prevent and counteract criminal activity.

The Money Laundering Act adopts a risk-based approach. Bearing in mind the company's business model and the company's specific focus on the gambling industry, it is Finansinspektionen's opinion that it is of the utmost importance for the company to take decisive action to manage the elevated risk of money laundering and terrorist financing that the gambling industry presents for the company's operations.

Finansinspektionen's investigation has revealed significant deficiencies in Trustly's compliance with the money laundering regulatory framework in

virtually every area covered by the investigation. The deficiencies that have been identified have resulted in the company consistently violating its obligations under the Money Laundering Act and the Money Laundering Regulations, which has increased the risk of Trustly and the financial system being used for money laundering and terrorist financing. These violations cannot be considered negligible.

There are no grounds for refraining from intervening as a result of Trustly's objection, stating that there was a valid excuse or that the deficiencies were not reprehensible. However, Finansinspektionen returns to section 5.4 and the issue as to whether Finansinspektionen's previous investigation of Trustly has an impact on the choice of intervention in the section relating to Trustly's failure to treat end users as customers.

Trustly has also stated that there are grounds to refrain from intervening due to the fact that the company has now taken, and plans to take, measures to rectify the deficiencies. However, Finansinspektionen believes that this is not possible due to the nature of the violations. It is the authority's position that it can only refrain from intervention if the nature of the violations is less serious (cf. Government Bill 2006/07:115 p. 500).

It is also true that no other authorities have taken measures against Trustly as a result of these violations. It is Finansinspektionen's position that on the whole the violations that have been identified are of such a nature that there are grounds to intervene against Trustly.

5.4 Choice of intervention

When choosing its intervention, Finansinspektionen has to take into account, inter alia, the severity of the violations and their duration. Special consideration must be taken of any damage that has been caused and the degree of responsibility.

Corresponding provisions in other business legislation for financial markets state that special consideration must also be taken to the nature of the violation and to its concrete and potential effects on the financial system: see, for example, Chapter 15 Section 1b first paragraph of the Banking and Financing Business Act (2004:297); and Chapter 25 Section 2 first paragraph of the Securities Market Act (2007:528). These circumstances are therefore not mentioned in Chapter 8 Section 9 first paragraph of the Payment Services Act. However, the legislative history makes it clear that the list in this provision and in Section 9a of this chapter is only indicative and that all circumstances must be taken into account when choosing an intervention and determining the administrative fine (Government Bill 2016/17: 173 p. 395 with further reference to pp. 373). There is therefore nothing to prevent consideration being taken, for example, to the nature of the violation and the concrete and potential effects on the financial system when choosing an intervention under the Payment Services Act.

The circumstances in this case are such that the violations resulting from Trustly not treating the end users as customers need to be dealt with individually and separately from the other violations.

5.4.1 Intervention through an injunction

The fact that Trustly has not treated the end users as customers when applying the money laundering regulatory framework has resulted in the company flagrantly violating its obligations pursuant to a number of provisions in the Money Laundering Act. As Finansinspektionen found in section 4.1.5, the violations have resulted in the end users, who make up the majority of the company's payment service users, not being included in the general risk assessment, not being assigned a risk class, not being covered by procedures and guidelines or not being covered by customer due diligence measures. Although Trustly has monitored the end users to some extent, this monitoring has been inadequate, as shown in section 4.6.

The deficiencies therefore applied to all end users, who comprise the majority of Trustly's payment service users. They have also applied to several central parts of the money laundering regulatory framework. Consequently, Trustly has actively ensured that the money laundering regulatory framework has not had an impact on its primary activities. This is something that is clearly serious.

As Finansinspektionen has stated in previous decisions, if there are systematic deficiencies or deficiencies of a more reprehensible nature against central parts of the money laundering regulatory framework, the only intervention would normally be to revoke the authorisation or alternatively to issue a warning, if this is considered to be sufficient. However, an overall assessment must be made on a case-by-case basis (Finansinspektionen's decision of 18 June 2020 in case FI Ref. 19-2342). The authority makes the same assessment in this case and finds that the nature of the violations is such that the violations should normally be assessed as being serious. What has emerged about their duration and their potential impact on the financial system would indicate the same.

The question is rather to what extent this assessment is to be influenced by the objection raised by Trustly, which has stated that the company has acted in good faith when assessing that end users are not customers, inter alia, based on Finansinspektionen's decision in a previous supervision case (FI Ref. 13-4173).

In the previous case referred to by Trustly, Finansinspektionen investigated the company's compliance with the then payment service and money laundering regulatory framework and the operations that the company conducted at that time. In its verification letter to the company, Finansinspektionen presented, inter alia, observations relating to Trustly's view of who its customers were. In its response to the verification letter, Trustly stated that the company considered that there was no customer relationship between the company and the end users, that the end users did not enter into a direct contractual relationship with Trustly, and that the contractual relationship that existed was between the end users and

the corporate customer. On 14 April 2015 Finansinspektionen decided to close this case without taking any action. The decision did not give any explanation as to why this case was closed. However, a note in Finansinspektionen's case management system actually states that the case was closed due to the fact that there had been no communication over a long period of time; however, it appears as though Trustly was not informed of this explanation.

When choosing the intervention, special consideration must be given to the degree of responsibility. Since no explanation was given as to why Finansinspektionen decided to close the case and apparently nothing else was communicated to Trustly, Trustly could be considered to have rightly perceived that the authority had no objection to the company's view that it did not have a customer relationship with the end users. It is Finansinspektionen's opinion that this therefore constitutes a circumstance that results in Trustly's behaviour being considered clearly less reprehensible than would otherwise have been the case (cf. Government Bill 2013/14:228 p. 240). This has such a mitigating impact on the assessment that in spite of everything the violations cannot be considered to be serious. The choice of intervention for the violations resulting from Trustly not treating end users as customers is therefore between ordering the company to take measures to rectify the situation and issuing the company with a remark.

Even when deciding between these two options, Finansinspektionen believes that there is reason to consider the decision to close the previous supervision case. There are also reasons to take into consideration the fact that Trustly no longer stands by its assessment, and that the company has applied and intends to apply measures to fully treat the end users as customers when applying the money laundering regulatory framework. When making an overall assessment of everything that has been stated above, Finansinspektionen considers that the most appropriate intervention is to issue the company with an injunction to take measures set out in the decision to rectify the situation.

It is Finansinspektionen's assessment that it is reasonable to allow Trustly until 30 November 2022 to apply these measures. Finansinspektionen will follow up the implementation of these measures. Trustly must therefore report in writing to Finansinspektionen the measures that the company has taken as a result of this injunction and the way these measures have resulted in the company complying with the injunction.

5.4.2 Intervention by issuing a warning

Finansinspektionen's investigation has also highlighted significant deficiencies that have not resulted from Trustly not treating end users as customers. These deficiencies have also been attributable to the company's exposure to the gambling industry and the risk this has presented to Trustly. Section 4.5 shows that the direct debit customers in Finansinspektionen's sample have executed a large number of transactions at a considerable value to and from gambling companies. In addition, Finansinspektionen has noted that Trustly has had high

exposure to a high-risk industry through its business relationships with the gambling companies.

The investigation in this section summarises the following deficiencies. Trustly's general risk assessment has not included all of the products and services provided by the company, nor has it included an assessment of the geographical risk that direct debit customers present for the company. In several cases, Trustly has not had any procedures and guidelines in place for customer due diligence for direct debit customers. Finansinspektionen has identified deficiencies in risk classification and customer due diligence measures for all direct debit customers in the sample. Trustly had deficiencies in its customer due diligence measures for all of the gambling companies. Furthermore, the company's monitoring system has not been designed as required by the money laundering regulatory framework.

For the reasons set out in section 5.4.1, the choice of intervention must be made independently of Trustly's failure to treat and monitor end users as customers. When making its assessment, Finansinspektionen must therefore disregard the fact that the authority has also found Trustly to have violated its obligations in these respects.

In terms of the nature of these violations, Finansinspektionen makes the same considerations and assessments it made in section 5.4.1. The deficiencies that have been identified have resulted in Trustly violating its obligations under several central parts of the money laundering regulatory framework. These deficiencies relate to the company's general risk assessment, risk classification of customers, procedures and guidelines, customer due diligence measures and monitoring. Finansinspektionen has identified deficiencies for all of the customers in the authority's sample. These deficiencies must undoubtedly be considered to be systematic.

These deficiencies have existed throughout the investigation period, which lasted for eight months. This means that the violations have existed for a relatively long period of time.

The investigation does not show that any damage has occurred as a result of these violations. The violations have not had any concrete effects on the financial system either. On the other hand, they have presented a clear risk that Trustly and the financial system could have been used to an increasing extent for money laundering and terrorist financing. This is particularly true when considering Trustly's risk exposure and the company's role in the payment chain, that can almost be compared to being a hub between the banks and the gambling companies.

Contrary to the assessment in section 5.4.1, there are no special circumstances for these violations that would mean that Trustly has a lesser degree of responsibility.

As a whole, Finansinspektionen finds the violations that have been identified to be serious.

As Finansinspektionen assesses some of these violations to be serious, the authority must consider revoking Trustly's authorisation. Revoking the authorisation of a payment institution is a very powerful intervention and must only take place if there are strong grounds to do so. It should be possible to issue a warning if there are circumstances for revoking the authorisation, but where a warning in an individual case is considered to be a sufficient measure (cf. Government Bill 2002/03:139 p. 383).

Finansinspektionen has not previously decided to issue Trustly with a sanction. The company has not facilitated the authority's investigation in such a way that it affects this assessment, nor has it quickly ceased with the violation after it was pointed out by Finansinspektionen. This means that there are no aggravating or mitigating circumstances pursuant to Chapter 8 Section 9a of the Payment Services Act to take into consideration.

Additional circumstances that would make a warning a sufficient measure is if the payment institution is not expected to repeat the violation and that the prospects for this institution are therefore good. 2002/03:139 pp. 382).

Trustly has presented measures that the company has applied and is planning to apply. As well as the measures to rectify the deficiencies themselves, it has also presented measures in the form of, inter alia, a directive for risk prioritisation by the Board of Directors and a strengthening of the organisation. Finansinspektionen's assessment is that overall, it appears that Trustly has applied and is planning to apply measures that will significantly reduce the risk of similar or new rule violations. Trustly may also be considered to be in a position to be able to implement these measures. Finansinspektionen therefore maintains its assessment that the prospect of Trustly rectifying the deficiencies and in the future comply with the regulatory framework is strong enough that issuing Trustly with a warning is a sufficient measure.

5.4.3 The amount of the administrative fine

As stated in section 5.4.2, the warning given to Trustly for the violations in that section will be combined with an administrative fine.

It has not been possible to determine whether Trustly has profited as a result of the violations and if so what gains it has made. A ceiling for the administrative fine is determined based on the company's or Group's turnover (see below) exceeding an amount that is the equivalent of EUR 5 million. This means that the 'ceiling' for the administrative fine that Trustly has to pay has to be determined on the basis of turnover.

In 2020 Trustly's turnover amounted to SEK 1,754 million, while the corresponding turnover at Group level amounted to SEK 1,975 million. Finansinspektionen states that the ceiling for the administrative fine is therefore SEK 197 million.

The size of the administrative fine is to be based on the severity of the violations. When Finansinspektionen determines the size of the administrative fine, the authority must give special consideration to the kind of circumstances that also have to be taken into account when choosing which sanction to issue, to the payment institution's financial position and, if it can be determined, the profit the institution has made as result of the violation. The fine that is determined must not be so high that the institution is subsequently not able to meet its capital requirements.

As stated previously, Finansinspektionen has not been able to determine whether Trustly has profited in any way as a result of the regulatory violations. Finansinspektionen presents its assessment of the violations in all other respects in section 5.4.2. The circumstances that are presented in that section as grounds for the choice of sanction are also the ones that have to be taken into consideration in determining the size of the administrative fine.

In view of what has been stated, Finansinspektionen sets the administrative fine at SEK 130,000,000. This administrative fine is not so high that Trustly will not be able meet its capital requirements as a result of the fine. The provision set out in Chapter 8 Section 15a second paragraph of the Banking and Financing Business Act, which states that the administrative fine may not be of such a size that the institution will subsequently not be able to meet the requirements set out in Chapter 3 Section 2 of the same act, therefore does not affect the size of the fine.

The administrative fine will accrue to the Swedish Government and is invoiced by Finansinspektionen after the decision enters into force.

FINANSINSPEKTIONEN

Sven-Erik Österberg
Chairman of the Board of Directors

Josephine Hedström
Legal Counsellor

Decisions in this case were made by the Board of Directors of Finansinspektionen (Sven-Erik Österberg, Chair, Maria Bredberg Pettersson, Peter Englund, Astri Muren, Stefan Nyström, Mats Walberg, Charlotte Zackari and Erik Thedéen, Director General) following a presentation by Legal Counsellor Josephine Hedström. Eric Leijonram, Chief Legal Counsel, Malin Schierenbeck, Deputy Director, Petra Bonderud, Deputy Director, Filip Lindahl, Legal Counsellor, and Erik Johansson, Supervisor, also participated in the final proceedings in the case.

Appendices
Appendix 1 – How to appeal
Appendix 2 – Applicable provisions

Copy: Trustly Group AB's CEO

N O T I F I C A T I O N R E C E I P T

Finansinspektionen
Box 7821
SE-103 97 Stockholm Sweden
[Brunnsgatan 3]
Tel +46 8 408 980 00
Fax +46 8 24 13 35
finansinspektionen@fi.se
www.fi.se

FI Ref. 20-20967
Notification No. 1

Warning, administrative fine and injunction

Document:

Decision on a warning, administrative fine and injunction to Trustly Group AB announced on **22 February 2022**

I have received the document on this date.

. . . . . .
DATE

. . . . . .
SIGNATURE

. . . . . .
NAME IN BLOCK CAPITALS

. . . . . .
NEW ADDRESS (IF APPLICABLE)

. . . . . .

. . . . . .

. . . . . .

This receipt must be returned to Finansinspektionen **immediately**. If the receipt is not returned, the notification may be issued in another manner, e.g. via a court officer.

Do not forget to **specify the date of receipt**.

Appendix 1 – How to appeal

It is possible to appeal the decision if you consider it to be erroneous by writing to the Administrative Court. Address the appeal to the Administrative Court in Stockholm, but send the appeal to Finansinspektionen, Box 7821, 103 97 Stockholm or finansinspektionen@fi.se.

Specify the following in the appeal:

- Name, personal ID number or corporate ID number, postal address, email address and telephone number
- The decision you are appealing against and the case number
- What change you would like and why you believe the decision should be changed.

If you engage an legal representative, specify the name, postal address, email address and telephone number of the legal representative.

Finansinspektionen must receive the appeal within three weeks from the day you received the decision.

If the appeal was received on time, Finansinspektionen will assess whether the decision will be changed and then send the appeal, the documents in the appealed case and the new decision, if relevant, to the Administrative Court in Stockholm.

Appendix 2 – Applicable provisions

Money laundering regulatory framework

Definitions

Chapter 1 Section 8(1) of the Act on Measures against Money Laundering and Terrorist Financing (2017:630) (Money Laundering Act) states that a business relationship refers to a commercial relationship that is expected at the time it is established to have a certain permanence. Chapter 1 Section 8(4) of the Money Laundering Act states that a customer is a person who has entered into or is about to enter into a contractual relationship with an obliged entity.

General risk assessment

Chapter 2 Section 1 first paragraph of the Money Laundering Act states that an obliged entity must assess the ways in which the products and services it provides in its operations may be used for money laundering or terrorist financing and the extent of this risk (general risk assessment). The second paragraph states that this general risk assessment has to take into consideration the kinds of products and services that are provided, the customers and the distribution channels, and any geographical risk factors. Consideration also has to be taken of any information that emerges when the obliged entity reports suspicious activities and transactions, and information about the approach to money laundering and terrorist financing and other relevant information provided by authorities.

Chapter 2 Section 2 first paragraph of the Money Laundering Act states that the scope of the general risk assessment must be determined based on the size and nature of the obliged entity and the risks of money laundering and terrorist financing. The risk assessment must be designed so that it can serve as a basis for the obliged entity's procedures, guidelines and other measures to prevent money laundering and terrorist financing.

Chapter 2 Section 1 third paragraph of the Money Laundering Regulations states that a company must update its general risk assessment before it offers new or significantly changed products or services, enters new markets or makes other changes affecting its operations.

Risk assessment of customers

Chapter 2 Section 3 first paragraph of the Money Laundering Act states that an obliged entity must assess the risk of money laundering or terrorist financing that may be associated with the customer relationship (the customer's risk profile). The customer's risk profile must be determined based on the general risk assessment and the obliged entity's knowledge of the customer. The second paragraph states that when it is necessary to determine the customer's risk profile, the obliged entity must take into consideration the circumstances

referred to in Sections 4 and 5 and regulations that are issued pursuant to the act, as well as other circumstances that affect the risk that may be associated with the customer relationship in the individual case. The third paragraph of this provision states the customer's risk profile must be followed up during continuous business relationships and changed when there is reason to do so.

Procedures and guidelines

Chapter 2 Section 8 first paragraph of the Money Laundering Act states that an obliged entity must have documented procedures and guidelines in place for its customer due diligence measures, and monitoring and reporting, as well as for processing personal data. The second paragraph states that the procedures and guidelines must be continually adapted to new and changed risks of money laundering and terrorist financing. The third paragraph of the provision states that the scope and content of the procedures and guidelines must be determined based on the obliged entity's size, nature and the risks of money laundering and terrorist financing that have been identified in the general risk assessment.

Customer due diligence

Ban on business relationships and transactions

Chapter 3 Section 1 first paragraph of the Money Laundering Act states that an obliged entity may not establish or maintain a business relationship or execute occasional transactions if the obliged entity does not have sufficient knowledge of the customer to be able to:

1. manage the risk of money laundering or terrorist financing that may be associated with the customer relationship; and
2. monitor and assess the customer's activities and transactions pursuant to Chapter 4 Sections 1 and 2 of the Money Laundering Act.

Situations that require customer due diligence

Chapter 3 Section 4 of the Money Laundering Act states that an obliged entity must apply customer due diligence measures when establishing a business relationship.

Chapter 3 Section 4 second paragraph of the Money Laundering Act states that if the obliged entity does not have a business relationship with the customer, customer due diligence measures must be applied:

1. for occasional transactions amounting to the equivalent of EUR 15,000 or more;
2. transactions that are below an amount that is the equivalent of EUR 15,000 and that the obliged entity realises or should have realised have a link with one or more other transactions and that total this amount; and
3. when executing the transfers of funds referred to in Article 3(9) of Regulation (EU) 2015/847 of the European Parliament and of the

Council of 20 May 2015 on information accompanying transfers of funds and repealing Regulation (EC) No 1781/2006, if the transfer exceeds an amount that is the equivalent of EUR 1,000.

Identification and checks of the customer

Chapter 3 Section 7 of the Money Laundering Act states that an obliged entity must identify the customer and check the customer's identity through identity documents or register extracts, or through other data from an independent and reliable source.

If the customer is represented by a person who claims to act on behalf of the customer, the obliged entity must check this person's identity and authorisation to represent the customer.

Chapter 3 Section 9 first paragraph of the Money Laundering Act states that checks of the customer's and the beneficial owner's identities must be completed before establishing a business relationship or executing occasional transactions.

Chapter 3 Section 10 of the Money Laundering Act states that an obliged entity must assess whether the customer or the customer's beneficial owner is a person in a politically exposed position, or a family member or close associate of such a person.

Chapter 3 Section 11 of the Money Laundering Act states that an obliged entity must check whether the customer is established in a country outside the European Economic Area (EEA) that the European Commission (Commission) has identified as a high-risk third country.

Information about and follow-up of business relationships

Chapter 3 Section 12 of the Money Laundering Act states that an obliged entity must obtain information about the purpose and nature of the business relationship.

Chapter 3 Section 13 first paragraph of the Money Laundering Act states that an obliged entity must continually and, if necessary, follow up continuous business relationships in order to ensure that its knowledge of the customer pursuant to Sections 7, 8 and 10–12 of the Money Laundering Act is up-to-date and sufficient to manage the assessed risk of money laundering or terrorist financing.

Customer due diligence measures required on a case-by-case basis

Chapter 3 Section 14 of the Money Laundering Act states that checks, assessments and investigations pursuant to Sections 7, 8, and 10–13 of the

Money Laundering Act must be carried out to the extent this is required based on the customer's risk profile and other circumstances.

Enhanced measures in the event of high risk

Chapter 3 Section 16 first paragraph of the Money Laundering Act states that if the risk of money laundering or terrorist financing that may be associated with the customer relationship is assessed as being high, much more extensive checks, assessments and investigations must be carried out pursuant to Chapter 3 Sections 7, 8 and 10–13 of the Money Laundering Act.

Chapter 3 Section 16 second paragraph of the Money Laundering Act states that the measures in such a case must be supplemented with the additional measures that are required to combat the high risk of money laundering or terrorist financing. These measures may refer to obtaining additional information about the customer's business operations and its financial situation, and data about where the customer's financial resources come from.

Chapter 3 Section 17 first paragraph of the Money Laundering Act states that enhanced measures pursuant to Chapter 3 Section 16 of the Money Laundering Act must be applied for business relationships or occasional transactions when the customer is established in a country outside the EEA that the European Commission has identified as a high-risk third country.

Monitoring

Chapter 4 Section 1 first paragraph of the Money Laundering Act states that an obliged entity must monitor continuous business relationships and assess occasional transactions in order to detect any activities and transactions that:

1. deviate from what the obliged entity has cause to expect, based on the knowledge it has of the customer;
2. deviate from what the obliged entity has cause to expect based on the knowledge the institution has about its customers, the products and services it provides, the data submitted by the customer and other circumstances; or
3. do not deviate as described in points 1 or 2, but can be assumed to be linked to money laundering or terrorist financing.

Chapter 4 Section 1 second paragraph of the Money Laundering Act states that the focus and scope of the monitoring must be determined by taking into account the risks that have been identified in the general risk assessment, the risk of money laundering and terrorist financing that may be associated with the customer relationship and any other information on the approach to money laundering or terrorist financing.

Chapter 4 Section 2 first paragraph of the Money Laundering Act states that if any deviations or suspicious activities or transactions are detected pursuant to Section 1 or in any other way, an obliged entity must apply enhanced customer

due diligence measures pursuant to Chapter 3 Section 16 and other necessary measures to assess whether there are reasonable grounds to suspect that it involves money laundering or terrorist financing or that property otherwise derives from criminal activity.

Chapter 4 Section 2 second paragraph of the Money Laundering Act states that when an obliged entity believes that there are reasonable grounds to suspect that money laundering or terrorist financing is involved or that property otherwise derives from criminal activity, additional measures pursuant to the first paragraph do not need to be applied.

Chapter 6 Section 1 first paragraph of the Money Laundering Act states that an obliged entity must have procedures and guidelines in place for internal control. The second paragraph states that the obliged entity must have procedures for model risk management if it uses models for risk assessments, risk classification, monitoring or other procedures. It also states that the procedures for model risk management must aim to evaluate and ensure the quality of the models used by the obliged entity.

Chapter 2 Section 1 third paragraph of the Finansinspektionen's Regulations (FFFS 2017:11) regarding Measures against Money Laundering and Terrorist Financing states that a company must update its general risk assessment before it offers new or significantly changed products or services, enters new markets or makes other changes affecting its operations.

Chapter 6 Section 16 of Finansinspektionen's Regulations (FFFS 2017:11) regarding Measures against Money Laundering and Terrorist Financing states that an obliged entity must validate a model before using it. If substantial changes are made to a model, a new validation must be carried out.

Chapter 6 Section 17 of Finansinspektionen's Regulations (FFFS 2017:11) regarding Measures against Money Laundering and Terrorist Financing states that a company must produce a report on the results of the validation after each validation it carries out of the model.

Payment Services Act (2010:751)

Obligations of the payment service provider when providing payment services

Chapter 1 Section 4 of the Act on Payment Services (2010:751) (Payment Services Act) states that a money remittance is a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, or where such funds are received on behalf of and made available to the payee.

Chapter 5 Section 8 of the Payment Services Act states that when providing payment initiation services, the provider may not:

1. hold at any time the payer's funds;
2. store sensitive payment data of the payment service user;
3. request from the payment service user any data other than those necessary to provide the payment initiation service;
4. use, access or store any data for purposes other than for the provision of the payment initiation service as explicitly requested by the payer;
5. modify the amount, the payee or any other feature of the transaction.