GUIDE TO TRUSTLY'S RISK MANAGEMENT

Introduction

Trustly's Risk Management System consists of a range of default and configurable settings that Trustly has incorporated into its payment service which help merchants to control losses from payments for which the funds never settle as a result of operational and fraud risks, which will be explained below in more detail.

Fraud risks are mitigated by Trustly through a range of measures; these cannot be configured by partners or merchants.

However, *operational bank risks* can be controlled by partners on a merchant level in order to optimize the Trustly experience. Please see section "Operational Bank Risk Management" on how these settings should be configured. We recommend starting with the next section which explains the primary risks in order to manage your Merchants' risk settings.

What are the primary risks of Trustly's payment offering?

The primary risks associated with Trustly's payment offering differ from risks associated with card payments, primarily due to significant variation among banking infrastructures throughout Europe. While there are also some fraud risks, these are better mitigated by Trustly compared with card payments. The table below describes in more detail these two types of risks associated with online banking payments.

Operational Bank Risks	Fraud Risks
Operational Bank Risk from unsettled transactions stems from the different ways banks' systems process bank transfers. Primary causes of this are: • Certain banks permit consumers to cancel authorized transactions before the funds leave the consumer's account • Certain banks do not process transactions instantly nor do they reserve the funds required for the transactions, creating a situation in which funds authorized for a Trustly payment may be spent elsewhere • Certain banks' infrastructure is simply less reliable and more prone to error	Fraud related to Trustly transactions usually is the result of end users' actions, deliberate or otherwise, which allow them to receive goods or services from the merchant without paying for them. Primary causes of this are: • Deliberate fraud: end users willfully deceiving merchants by exploiting banking systems' that allow consumers to cancel transactions • Phishing fraud: end users obtaining bank login credentials allowing them to make unauthorized transactions from another user's account • Friendly fraud: end users claiming a refund for a purchase they authorized themselves without malicious intent

How best to manage these risks?

Trustly's payment initiation services ("PIS") and account information services ("AIS") are built upon existing bank processing systems and inter-bank clearing and settlement infrastructures. Given that these systems' processing infrastructures still vary significantly between countries and between banks in their ability to process instantly and reliably, Trustly has developed its Risk Management service to help merchants balance instant payment experience for consumers with minimizing the risk of non-settlement for merchants.

Operational Bank Risk Management

Due to diverse bank infrastructure systems, bank payments can settle with different speeds and probabilities. Trustly's unique position in the flow of funds with receiving bank accounts provides a significant advantage over other bank transfer providers. This is because Trustly can constantly monitor whether transactions from end user accounts do settle and can classify banks based on this. In addition to these bank classifications, Trustly incorporates limits which merchants can configure (Exposure Limits - explained further below) in order to more finely balance the mitigation of losses from unsettled transactions and providing an instant end user experience.

Bank classification

Trustly classifies all banks to determine whether they are optimised for Trustly's service since online capabilities and behaviour vary from bank to bank e.g. the ability for users to cancel completed transactions, whether funds are reserved on the user's bank account or not.

Trustly uses two types of bank classifications after a sufficient number of transactions have been completed for each bank:

Optimised bank	Basic bank
A bank for which Trustly has experienced extremely low rates of non-settlement. These banks provide end users with an instant service and merchants with an extremely low probability of incurring losses.	A bank for which Trustly has experienced a relatively high rate of unsettled transactions. These banks are not optimised for Trustly's service and so by default don't provide an instant experience for end users

Exposure limits

Exposure limits are set depending on the bank classification (mentioned above) to control losses from unsettled transactions. These limits set the maximum cumulative order value at which the merchant is instantly notified to release the goods or services to the end user e.g. when the merchant should process the order and ship the goods to the end user, credit the end user's account etc. Cumulative order values surpassing the set exposure limit will not trigger instant notifications to release the goods, but rather notifications will be delayed until the funds have settled to Trustly's receiving bank account.

How do bank classifications and exposure limits work together?

Bank classification	Default exposure limit (1)	Credit notification	Possibility of loss	Liability of losses
Optimised banks	Up to €1,000 / €2,200 (SE, FI) / € 2,000 (EE, NL)	Instant	Yes	Merchant
	Anything above €1,000 / €2,200 (SE, FI) € 2,000 (EE, NL)	Delayed	No	
Basic banks	€0	Delayed	No	N.A
Note: 1. These are applied to the majority of banks, but not all.				

Trustly credit notifications

Credit notifications inform the merchant when to release the goods or services to the end user. The timing of these notifications is based on the bank classification of the end users' bank and the exposure limit set by the merchant.

1. Instant: sent immediately after the end user has completed the payment initiation up to the exposure limit set. As bank infrastructure varies from country to country, this notification can be sent before the funds have settled in Trustly's receiving bank accounts

2. Delayed: sent only after the funds have settled in Trustly's receiving bank accounts

More information on how the different processes work can be found in the appendix.

How to optimize exposure limits for your merchants?

Trustly's Risk Management service works as follows:

1. When sending Trustly the online Merchant Boarding Form, Partners confirm that they wish to keep the Default Exposure Limits, or specify that they wish us to configure bespoke Exposure Limits for the Merchant.

2. When Partners select Default Exposure Limits:

    a. Instant credit notifications will be sent for all Optimised Banks' (and Evaluation Banks' - see the Appendix for more details) transactions up to the Exposure Limits.

    b. Delayed credit notifications will be sent for all Basic Banks (i.e. the exposure limit will be set to 0 and credit notifications will only be sent once end users' funds settle into Trustly's receiving bank accounts).

c. Delayed credit notifications will be sent for all individual transactions exceeding the exposure limits

d. Delayed credit notifications will be sent when the cumulative value of all to-be-settled transactions from an individual bank account exceeds the exposure limit

3. When considering whether to keep the Default Exposure Limits or to have Trustly configure bespoke Exposure Limits, Partners and Merchants should consider the following:

Merchant Characteristics	Exposure Limit Approach	Example Industries
• Instant delivery of service is critical • Cost resulting from non-settlement is low or manageable	Higher Exposure Limits may increase conversion and improve user experience without meaningfully adding to Merchant risk	• Digital goods • Online gaming
• Instant delivery of service is critical • Revenue upside from instant delivery outweighs risk of increased loss	Higher Exposure Limits may increase conversion and improve user experience to a degree that outweighs any increase in loss rate	• Online gambling
• The most frequent transaction value is higher than the Default Exposure Limit	Higher Exposure Limits targeted to specific banks in specific countries may help optimise conversion and improve user experience in those countries without unduly increasing loss rates	• Travel
• Non-settlement of funds results in a significant direct loss to the Merchant	Lower or 0 Exposure Limits at Basic banks will help to minimize loss rates	• Physical goods • Travel • Financial services
• Lead-time from order to shipping is less critical • ATV or the most frequent transaction value is quite high	Lower or 0 Exposure Limits at Basic banks will help to minimize loss rates.	• High-value physical goods • Financial services

Why not eliminate all risk?

In an increasingly digital world, instant gratification is everything for consumers. To meet these demands online businesses have to provide an instant and seamless experience for their consumers whenever possible. Trustly's service provides the experience and flexibility for Partners and their Merchants to deliver a truly compelling bank transfer proposition despite the varying quality in bank infrastructure and online systems.

For banks that do not settle quickly, Trustly need to set the exposure limits above 0 in order for the service to feel instant for the end-user; slow transfers lower conversion rates as we inform consumers about the expected transaction speed during the consumer payment flow.

Fraud and Money Laundering Risk Management

Trustly performs multiple checks in order to prevent fraud and mitigate money laundering risk. You will find more information on "types of fraud" under the section "What are the primary risks of Trustly's payment offering" on page 2.

How do Trustly control Fraud and money laundering risk?

In order to mitigate fraud risk for end-users, Trustly's sophisticated fraud risk management tool performs multiple checks each time an end-user makes a purchase with Trustly and prevents fraud and money-laundering by;

- Running its own checks against PEP and sanctions lists on top of banks' stringent policies
- Not sharing end-user login credentials with Merchants
- Supporting the full range of bank-issued multi-factor authentication methods
- Maintaining our checks on consumers
    - Blacklists - blocks end-users who have been deemed to have commited fraud
    - Grey lists - when we see consumers with previously unsettled deposits, but we do not necessarily know the reason (intentional/unintentional), they will still be able to use Trustly's services, but we will mitigate risk of non-settlement by always waiting for settlement before sending a credit notification to the merchant
    - White lists - as part of our monitoring, we will unblock - or "white list" - customers where we conclude that a previous block/grey listing is no longer relevant.
    - Consistency checks - look for logical patterns in shopper and payment data, including geographical aspects

Appendix A:

Key definitions / Glossary

Given that Trustly's payment initiation services operates differently from card payments, there are a handful of terms that are necessary to understand in order to properly use Trustly's Risk Management services.

Basic Banks Banks for which Trustly has experienced a high rate of unsettled transactions, typically because customers of these banks are permitted to cancel transactions or because the banks don't reserve money following a Payment Initiation, and as a result experience higher unsettled rates.

Credit Notifications An API notification sent from Trustly to a Partner or Merchant to indicate either 1) that funds have arrived in Trustly's settlement account for the Partner or Merchant, or 2) that a deposit transaction has been initiated which is below the Exposure Limit for a given Merchant and consumer. Credit notifications can be sent instantly (for cases 1 and 2 above), but for basic banks, can take up to 1 or even on rare occasions 2 days following successful initiation of a payment of a Trustly transaction at a Merchant.

Default Exposure Limits In order to help Partners and Merchants quickly and easily optimise their consumers' experience and conversion rates using Trustly, we have developed a set of Default Exposure Limits that will be automatically applied to Partners' Merchants unless Partners wish to enable bespoke settings for their Merchants.

Delayed Credit Notifications These are Credit Notifications sent to Partners and Merchants only upon actual receipt by Trustly of the consumer's funds (Trustly Settlement). As such, Merchants using Delayed Credit Notifications to trigger release of goods/services will have virtually zero risk of loss; however, their speed of release of purchased goods will be up to 1 and in rare cases even two days later than when they use Instant Credit Notifications.

Evaluation Bank A new bank for Trustly, where we have not yet experienced adequate volume to determine if the Bank should be categorized as Optimised or Basic. For Evaluation Banks, Trustly recommends a relatively low Exposure Limit, and Trustly will reimburse Merchants for losses incurred at Evaluation Banks when the transaction value was below Trustly's Default Exposure Limit (see above).

Exposure Limit A configurable value that determines when Trustly will send Credit Notifications to Partners. Exposure limits can be set as low as 0 or as high as Merchants so desire. Payment initiations that are at or below the configured exposure limit for a bank will instantly trigger Credit Notifications to the Partner or merchant. Payment initiations that are in excess of the configured exposure limit will only trigger a Credit Notification once Trustly has actually received funds settlement from the consumer's bank account (typically between a few hours and T+1, though in rare cases, up to T+2). Note that Exposure limits are also cumulative, per consumer bank account. That is, two transactions from the same consumer bank account that have not yet settled to Trustly's collecting account will only trigger a Credit Notification for the second transaction once the cumulative amount of outstanding funds falls below the Exposure limit.

Instant Credit Notifications These are Credit Notifications immediately sent to merchants, or to Partners for forwarding to Merchants, in order to notify Merchants to release the goods purchased. Instant Credit Notifications are sent when 1) the transaction amount is below the configured Exposure Limit AND the cumulative value of to-be-settled transactions for a specific consumer bank account has not surpassed the Exposure Limit, or 2) funds have actually settled instantly to Trustly's settlement account (typically for markets where Trustly's settlement account is in the same bank as the consumer's sending account, or in markets where they have implemented an instant payment scheme such as SEPA Instant in Europe or Faster Payments in UK).

Loss Rate The proportion of all transactions which result in a loss when an Instant Credit Notification was sent by Trustly to the Partner, and consequently the purchased goods or services were provided to the consumer, but the consumer's payment did not settle to Trustly's settlement account.

Merchant Settlement This refers to the transfer of funds collected by Trustly to the Merchants. In the case of a Collecting Partner, Trustly does not undertake Merchant Settlement directly, as Merchant Settlement is between the Partner and the Merchant. However, in the case of a Technical Partner, Trustly will not undertake Partner settlement, and instead, Trustly will undertake Merchant Settlement directly with each individual Partner Merchant.

Optimised Banks Banks for which Trustly has experienced extremely low rates of unsettled transactions. These are banks for which Merchants can with confidence set their Exposure limits relatively high, due to their extremely low Loss Rates.

Partner Settlement This refers to the transfer of funds held by Trustly on behalf of Merchants to the designated settlement (corporate) account of a Collecting Partner (PSP). Partner Settlement can be set by Collecting Partners to happen on a daily, weekly or monthly basis, or on an ad hoc, "push" basis. Partner Settlement includes transfer of funds from all of a Collecting Partner's Merchants (consolidated settlement).

Pending Notifications An API notification sent from Trustly to a Partner to indicate that a Trustly payment transaction has been successfully initiated at a Merchant. Pending Notifications happen instantly – within seconds—of a payment being successfully initiated. However, they do not indicate that Merchants should release the goods purchased, nor do they indicate that Trustly has received the funds sent.

Trustly Settlement This refers to Trustly actually receiving a consumer's funds in its collecting account. If it has not happened already, Trustly settlement triggers a Credit Notification to the Partner.