



# Project Indicators

An opportunity to detect  
payments for livestreamed  
child sexual abuse



# Table of contents

<b>Glossary.....</b>	<b>3</b>
<b>Background.....</b>	<b>3</b>
<b>Objective.....</b>	<b>4</b>
<b>Our method and activities.....</b>	<b>4</b>
<b>Case study.....</b>	<b>5</b>
<b>Test runs.....</b>	<b>6</b>
<b>Reporting of suspicious transactions.....</b>	<b>6</b>
<b>Indicators based on the case study.....</b>	<b>7</b>
<b>Perpetrator.....</b>	<b>7</b>
<b>Financial indicators.....</b>	<b>8</b>
<b>Results of the test runs.....</b>	<b>9</b>
<b>Reporting to the Financial Intelligence Unit.....</b>	<b>10</b>
<b>Conclusions.....</b>	<b>10</b>
<b>Compiled list of indicators .....</b>	<b>11</b>

## Glossary

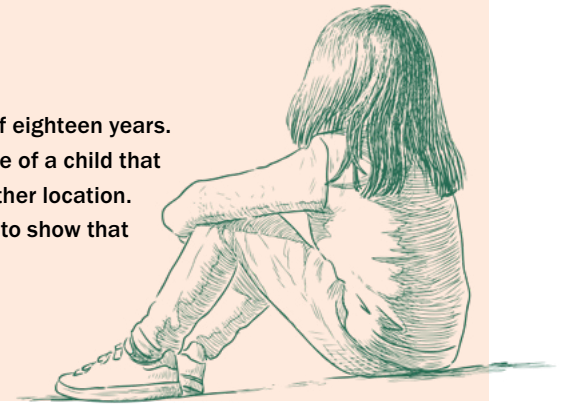
**CHILD/CHILDREN** – Every human being below the age of eighteen years.

**LIVESTREAMED CHILD SEXUAL ABUSE** – A sexual abuse of a child that is documented and livestreamed to a perpetrator in another location.

**INDICATOR** – A measurement or value that can be used to show that something is a certain way.

**TOKENS** – A digital currency.

**CSE** – Child sexual exploitation.



## Background

**CHILD SEXUAL EXPLOITATION** is a widespread crime that can extend across country borders. A clear example of this is when children are exposed to so-called livestreamed child sexual abuse. The concept of livestreamed child sexual abuse can include different types of exposure. For example, it can refer to situations where children are induced by a perpetrator to perform sexual acts on themselves. These situations are then livestreamed to the perpetrator through for example a webcam.

It can also refer to situations where a perpetrator is in another country and, for a fee, orders a sexual abuse of a child to take place in another country. The abuse is then livestreamed to the perpetrator via webcam. In these situations, the child is subjected to sexual abuse by one or more perpetrators who are in the same location as the child. However, despite the distance to the perpetrator who ordered the crime, he or she is typically very much involved during the abuse. This can be through instructions on how the act should be carried out as well as pay more money during the abuse.

ECPAT has worked to prevent livestreamed child sexual abuse – both at a national level and through international collaborations – for a long time. Since the exposure involves a perpetrator paying a sum of money for the crime, it means that a transaction must take place which should therefore also be traceable.

ECPAT Sweden's Financial Coalition (the Financial Coalition) was initiated with the aim of working together with actors from the financial sector to prevent the actors' services from being misused for payments for sexual abuse of children. The Financial Coalition currently consists of 14 banks, Softronic and representatives from the National Operations Department of the Police (NOA). In 2020, the Financial Coalition initiated Project Indicators with the objective of jointly hinder and prevent payments for livestreamed child sexual abuse from taking place.

## Members of ECPAT Sweden's Financial Coalition

Avanza

Danske Bank

DNB

Forex

Handelsbanken

ICA Banken

Ikano Bank

Klarna Bank

Länsförsäkringar Bank

Marginalen Bank

Nordea

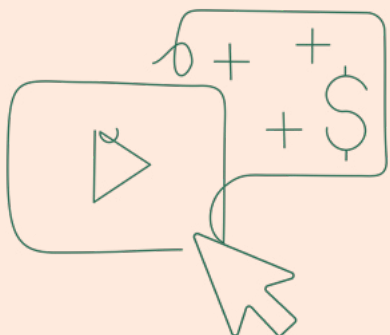
SEB

Skandiabanken

Swedbank

Softronic

Nationella operativa  
avdelningen inom  
polisen (NOA)

## Objective

**PROJECT INDICATORS** aims to identify indicators and working methods that banks can use in their operations to detect payments made for livestreamed child sexual abuse.

## Our method and activities

**AS PART OF INITIATING** the project a working group was set up consisting of members from the Financial Coalition as well as representatives from ECPAT. Initially, the project encountered obstacles in the form of banking secrecy and its impact on the ability of banks to report transactions suspected of stemming from the purchase of livestreamed child sexual abuse. The issue caused the project to be put on hold for a period. In 2023, the project had a restart together with a new working group. The new working group consisted of representatives from ECPAT, a bank, Softronic and the Financial Intelligence Unit.



## Case study

**IN EARLY 2023**, ECPAT conducted a case study with the aim of identifying indicators that could be relevant for detecting payments for livestreamed child sexual abuse. The case analysis was made based on a selection of court cases based on predetermined criteria. The criteria were that the offender should be suspected of crimes involving the purchase of livestreamed child sexual abuse and that the verdict or preliminary investigation should include information about the payment method and amount paid. It was also of interest to look at certain cases concerning related crimes, such as depicting of child sexual abuse material, acquiring of child sexual abuse material and dissemination of child sexual abuse material.

### In total, the following 11 judgments from Swedish courts were analyzed:

1. Hovrätten för Nedre Norrland 2018-05-22 B 284–18 (Östersunds TR B 1116–17)
2. Hovrätten för Västra Sverige 2019-02-22 B 1082–19 (Halmstads TR B 665–18)
3. Hovrätten över Skåne & Blekinge 2013-04-12 B 213–13 (Hässleholms TR B 610–12)
4. Kristianstads TR 2011-12-27 B 276–11
5. Malmö TR 2021-04-28 B 6250–20
6. Svea hovrätt 2022-04-06 B 1095–22 (Norrtälje TR B 495–21)
7. Skaraborgs TR 2022-09-29 B 1206–21
8. Svea hovrätt 2018-04-16 B 11734–17 (Uppsala TR B 3216–16)
9. Svea hovrätt 2019-10-22 B 8435–19 (Sthlm TR B 11206–18)
10. Uppsala TR 2015-02-19 B 1189–14
11. Södertörns TR 2023-03-28 B 401–22

Of these 11 judgments 9 were of more relevance based on the purpose of the case study.

Based on the above court cases, indicators such as the typical case of offender, payment method and amount paid could be identified.



## Test runs

**AFTER THE CASE STUDY** had been established, the indicators from it formed the basis for the data analysis carried out by Softronic as a next step in the project. The analysis was done on anonymized transaction data from a bank. Some customer information such as age and gender were also considered in the analysis.

Initially, the data analysis was done manually to investigate whether combinations of the indicators could generate an outcome of customers that were considered interesting for further investigation. Early in the analysis phase, it could be established that the success rate was good and that the conditions existed for a more automated model.

As a follow-up step, the analysis was broadened to investigate whether it was possible to identify

more transactions. The hit picture was naturally worsened when the analysis was broadened, but still within an acceptable level. In dialogue with the participating bank in the working group, some of the indicators could either be expanded or refined so that the analysis was more accurate.

The customers related to detected transactions that the data analysis resulted in were communicated to the participating bank in three rounds. To not affect the bank's investigation, information about why these customers were detected was not disclosed at the handover. The bank has subsequently investigated the customers' transactions according to their usual routine, with an extra focus on identifying transactions or patterns that could be linked to child sexual exploitation.

## Reporting of suspicious transactions

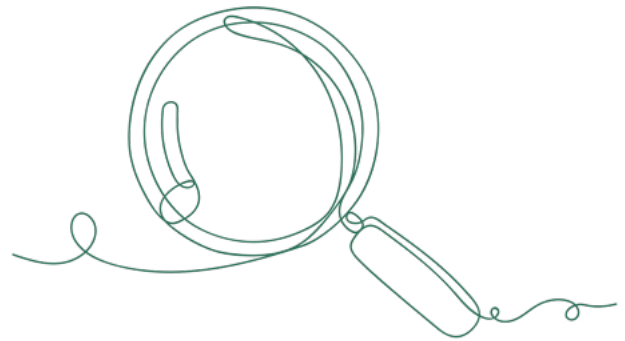
**A QUESTION IN ADDITION** to identifying a working method for detecting transactions that the working group had to consider, was how the reporting of this type of transaction should be done to the Financial Intelligence Unit. The question was prompted by the fact that the category of crime that payments related to the sexual exploitation of children constitute, typically deviates to some extent from the type of transactions that are

normally reported. The Financial Intelligence Unit is primarily tasked with investigating transactions related to terrorism financing and money laundering. However, the latter category can also be relevant in the case of payments linked to sexual exploitation of children. The working group therefore discussed possible ways to mark these transactions in connection with reporting to the Financial Intelligence Unit.



## Indicators based on the case study

**A PREREQUISITE** for being able to detect payments that go to livestreamed child sexual abuse is to know what characterizes these payments. Through the case study carried out by ECPAT, indicators for type of perpetrator, amount paid, and the payment method used could be identified.



### Perpetrator

**THE TYPICAL CASE** of a perpetrator who orders and pays for livestreamed child sexual abuse according to the case study is a man between 37 and 50 years old. The perpetrator is typically in Sweden and orders a livestreamed sexual abuse that takes place in the Philippines.



## Financial indicators

**IN THE COURT CASES**, there were mainly two different types of payment methods used:

1. Tokens via websites
2. Payments via different payment providers

The most frequently used payment method was the purchase of tokens on various websites. Tokens act as a digital currency linked to a specific platform. They can be used to make purchases on the platform or as tips during the abuse. In cases where tokens were used as a payment method it was not identified from the transaction as such, but from other evidence in the case. In cases where tokens had been used, the offenders either made the payments via bank transfers from their Swedish bank or via their debit card.

Transfers via Western Union, PayPal, and WorldRemit were the second most common payment method after purchasing tokens. These transfers were usually made to someone in the Philippines. The least frequent payment method was the use of payment providers such as XOOM and Remitly. In cases where these payment methods were used, the transfers were mainly made via the perpetrator's bank card.

The amount that the perpetrator typically paid for a livestreamed sexual abuse varied somewhat in the court cases. However, it was possible to establish that higher amounts than 400 SEK were less common, although there were a few transactions of around 1 000 SEK in some of the court cases. When buying tokens, it was common for the offender to buy several at the same time. A token typically cost around 1 SEK each.

Overall, based on the case study, a livestreamed sexual abuse usually costs somewhere between 90 and 300 SEK.



### Payment methods

#### TOKENS

- Payments via bank transfers or debit card

#### TRANSFER VIA DEBIT CARD TO:

- Western Union
- WorldRemit
- Paypal
- XOOM
- Remitly
- Often to a person in the Philippines

### Amount paid

#### COST PER TOKEN 1 SEK EACH

- Payments made in lump sums of – for example 200-400 SEK several times a week

#### AMOUNT PER LIVESTREAMED ABUSE

- Between 90 and 300 SEK





## Results of the test runs

**THE TEST RUNS** that were carried out based on the indicators from the case study resulted in a number of hits on customers who were of interest and could be reported on to the participating bank. When a suspicion of child sexual exploitation arose, these customers and transactions were reported to the Financial Intelligence Unit.

In cases where the customer was not reported to the Financial Intelligence Unit with suspicion of sexual exploitation of children, it was because the customers in question had a rational explanation for their transactions, such as holiday trips, dual citizenship, or studies abroad.

**Out of the customers who were reported to the Financial Intelligence Unit with suspicion of sexual exploitation of children, the following indicators could be noted linked to the individuals themselves:**

- Men
- Born in the 1950s, 1960s and 1970s
- Conduct transactions abroad, primarily through international apps, in parallel with transactions in Sweden
- Provides a non-response to a transaction request made by the bank

In addition, additional common indicators have been noted linked to card purchases and transfers made to recipients such as WorldRemit, Western Union, Tiktok, Wise, Grab, Food Panda, PayPal, Remitly and Onlyfans. In general, the reported customers have completed a combination of transactions to several of the recipients mentioned above, which e.g. can be a combination of card purchases to Tiktok, WorldRemit and Grab. The number of transactions per recipient can vary greatly, ranging from 10 to over 600 over a one-year period. In many cases, the card purchases are made late at night, at night or early in the morning. This can be an indication that the recipient is in a different time zone. The amounts vary from a few SEK to 5 000 SEK and more. In terms of country, the Philippines is the most common when it comes to card purchases via Grab and Food Panda. The bank has not been able to identify which countries card purchases to WorldRemit, Wise and Western Union have gone to.





## Reporting to the Financial Intelligence Unit

**TO OBTAIN A UNIFORM** reporting to the Financial Intelligence Unit for the category that transactions with suspected links to the sexual exploitation of children fall into, the working group concluded that banks should mark this type of report with the heading

**“suspected CSE” (child sexual exploitation).** The marking enables the Financial Intelligence Unit to notice this type of reporting in an easier way. The marking was used during the course of the project when reports were made and proved to be successful.

## Conclusions

**THE WORKING GROUP’S** widespread range between sectors has meant a crucial sharing of experiences that has enabled the project to move forward. This has contributed to the possibility of having cross-sectoral dialogues, which has resulted in a uniform way of reporting transactions suspected of stemming from child sexual exploitation to the Financial Intelligence Unit. This means a step in the right direction for the police to become aware of this type of crime and thus also be able to investigate it.

Another success factor from the project was that actual applicable indicators for transactions related to livestreamed child sexual abuse could be identified. By putting the indicators

from the case study into practice via the test runs they could be further refined. The result of the test runs also helped to confirm the indicators as relevant, as the indicators made it possible to detect transactions where there was reason to suspect sexual exploitation of children.

The results of the project show that all the prerequisites are in place to both detect and make it more difficult to make transactions related to sexual exploitation of children. The project also highlights the important role the financial sector has in the work of preventing child sexual exploitation. It is therefore necessary that these actors also fulfill their responsibility and act.



## Compiled list of indicators

### PERPETRATOR:

- Man
- Born in the 1950s, 1960s, 1970s or 1980s

### TRANSACTION PATTERN:

- Transactions made abroad (typically the Philippines)
- Transactions through international apps
- Transactions to:
  - Western Union
  - WorldRemit
  - Paypal
  - XOOM
  - Remitly
  - Tiktok
  - Wise
  - Grab
  - Food Panda
  - Onlyfans
- 10-600+ transactions a year per recipient
- Tokens - Payments via bank transfers or debit card
- Transactions made late at night, at night or early in the morning
- A non-response to a transaction request made by the bank

### AMOUNT PAID:

- Tokens – 1 SEK each
- Livestreamed child sexual abuse – 90-300 SEK per stream
- 1 SEK to 5 000 SEK and more per transaction



# ECPAT Sweden's Financial Coalition

@ECPATSverige

+46 (0)8 598 920 00  
info@ecpat.se

[www.ecpat.se](http://www.ecpat.se)  
[www.ecpat.se/hotline](http://www.ecpat.se/hotline)  
[www.dittecpat.se](http://www.dittecpat.se)

Swisha din gåva till  
90 34 34 9  
Bankgiro: 903-4349

