BLACK WALLET

BLACK WALLET
RISK INDICATORS

POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation

Polisen
Swedish Police

The Black Wallet Risk Indicators is one of the end-products of the project. The Risk Indicators are accompanied with the Risk Indicators Report, which gives more thorough and detailed information as well as examples about the threats, vulnerabilities and red flags that the Black Wallet Project Group has identified in this document. The Black Wallet Risk Indicators are targeted to the Payment Service Providers (PSPs) and Financial Technology (Fintech) companies in order to help the companies realise, assess and mitigate risks that may arise in relation to their products and services.

The Black Wallet Project is an EU-funded, joint project between the Finnish and Swedish Financial Intelligence Units with support from other competent authorities from the respective countries. During the course of the project (March 2019 to February 2021), the aim has been to create an overall picture of the Fintech sector, especially focusing on products and services related to the transferring of funds. Ultimately, this has helped the law enforcement authorities and the private sector to prevent, detect and investigate terrorist financing (TF) and money laundering (ML).

Threats

Threats in the Black Wallet Risk Indicators cover the top level events and features that can be common to the whole industry. Threats can also be perceived as something that the companies may have limited ability to control with their risk mitigation measures. Threats are sprung from the playing field of the companies, such as obligations set by local or transnational authorities or the way customers use the products and services.

Compliance and legal obligations

- Challenges to collect Known Your Customer (KYC) and user/customer identification.
- Ability to identify customer-/client-specific risks when onboarding.
- Risks awareness; insufficient compliance and monitoring mechanisms (personnel, IT).
- Employee risk; internal misuses.
- Issues related to reporting to the Financial Intelligence Unit (FIU).

Fintech service specific features

Geographical coverage, speed and complexity of transactions.

Transparency and traceability of transactions

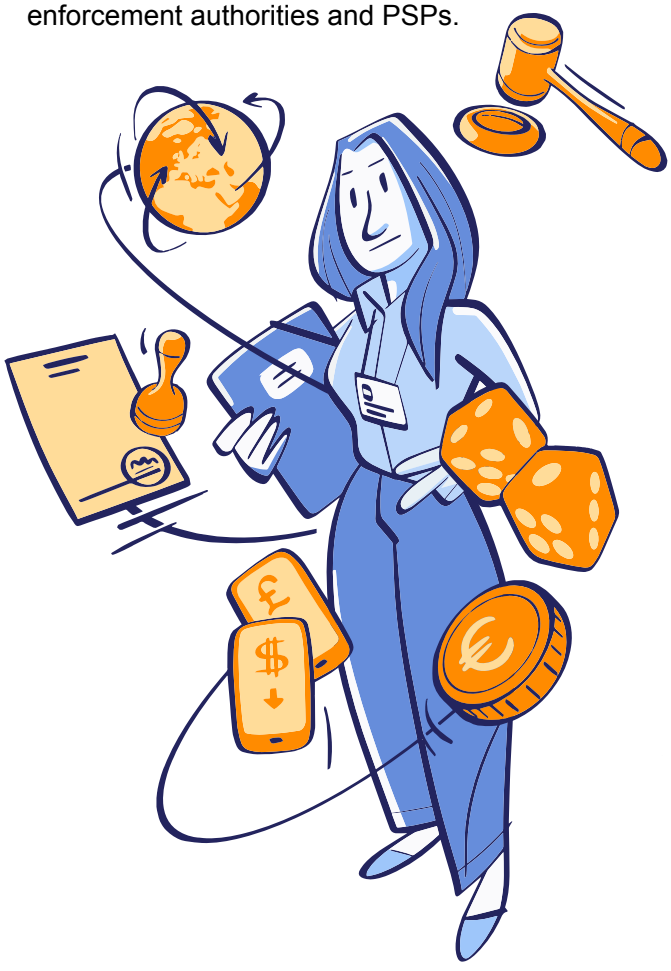
- Separation of data; data fragmentation to several actors.
- Outsourcing parts of the service.
- Handling of others' clients.

Illicit intentions of the PSP

- Founded to be used for illicit purposes.
- Investments from illicit sources to acquire control of the PSP.

Authorities

- Authorities may have difficulties in understanding the services and the flow of the transactions when tracing the assets.
- Inability to keep up with technology development.
- Information gathering may require information requests to several jurisdictions.
- Complex nature of the industry for both the supervisory and the investigative authorities.
- Lack of cooperation between the law enforcement authorities and PSPs.



Vulnerabilities

Vulnerabilities are characteristics in the PSPs themselves and in their connected or supportive services. The PSPs have the power to mitigate vulnerabilities to some extent by planning business operations and developing their products accordingly.

Product

- High-value activities; there are no adequate thresholds for transactions, payments, storing, loading or redemption, including withdrawal.
- Funding of the product can be done anonymously with cash, e-money, exemption-granted e-money products, or from unidentified third parties.
- Use of the product allows person-to-person transfers.
- Use of the product is suitable for services with a high risk of financial crime.
- Use of the product or service enables it to have a global reach, be used in cross-border transactions or in different jurisdictions.
- The product can be used by persons other than the customer.
- Client's user accounts: methods for changing information on a user account lack proper safeguards.

Distribution channel

- Customer funds account is related to the use of the product and may allow higher degree of anonymity and complexity if customer data doesn't travel with the transaction.
- Distribution channel provides a degree of anonymity.
- Service is provided entirely online without adequate safeguards.
- Service is provided through agents who have unusual turnover patterns compared to other agents in similar locations.
- Service is provided through agents who undertake a large proportion of business with payers or payees from jurisdictions associated with higher ML/TF risk.
- Service is provided through agents whose Anti Money Laundering/Counter Financing of Terrorism (AML/CFT) policies are inconsistent.
- Service is provided through an agent who is not from the financial sector and conducts another business as their main business.
- Service is provided through an overly complex payment chain that possibly involves different jurisdictions.
- Distribution through intermediaries that are not themselves obliged entities.

Distribution channel (continued)

- Data security or storage through third-party service providers.
- PSP is connected to several operationally independent service providers without mutual co-ordination in business.
- PSP does not receive the relevant information from the third party doing the KYC or monitoring.
- PSP cannot forward all of the relevant information accompanying the payment to the third party.
- Use of non-official intermediaries (no documentation, no webpages).

PSP's own characteristics and functions

- PSP is funded or receives funding to be used for illicit purposes.
- PSP does not verify if the actual user of the service is the customer.
- PSP has limited information about the customer/user of the product.
- PSP relies on the first phase of identification instead of constantly updating the KYC information of the customer.
- PSP does not have any face-to-face meetings with customer.
- PSP trusts unreliable sources of information or uses sources incorrectly.
- PSP can't access all data due to data fragmentation between different companies.
- PSP lacks the customer risk categorisation needed to mitigate and monitor risks.
- PSP's transaction monitoring is not timely or is delayed.
- PSP uses only static and fixed limits in monitoring.
- PSP is not looking for more complex patterns in transactions.

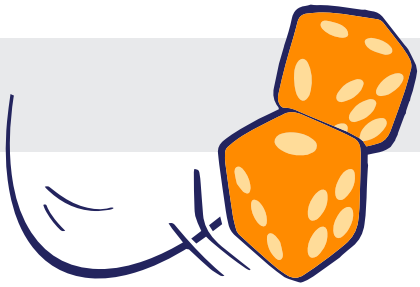
Red flags

Red flags – risks in the behaviour of PSP's customers – cover registering and KYC, customer profile and transactions. Registering and KYC refer to risks during the registration or while conducting KYC. Red flags related to the customer's profile are linked to customer behaviour that differs from regular product or service usage or indicates other abnormality compared to the intended use. Transaction red flags relate to transactions that customers initiate.

Registering and KYC

- Customer purchases and/or uses several e-money products from the same issuer.
- Product designed to be used by a single person appears to be used by several people.
- There are frequent changes in the customer's identification data.
- Product is not used for the purpose it was intended for.
- Customer owns or operates a business that handles large amounts of cash.
- Customer's business has a complicated ownership structure.
- Customer's needs might be better serviced elsewhere.
- Customer appears to be acting for someone else.
- Customer's use of the service is unusual.
- Customer appears to know little about the payee.
- Incoming transaction is not accompanied by the required information on the payer or payee.
- The amount sent or received is at odds with the customer's declared or expected financial situation.
- Registration is carried out using an anonymous or disposable email service
- Customer's contact information can be linked to several profiles.
- Customer's IP address and address of residence don't match.
- Origin of the funds is unclear.
- Documents provided by the customer for the customer due diligence process contain errors or are of poor quality.
- Indications that the customer is a Politically Exposed Person (PEP).
- Indications that the customer is on a sanction list, official freezing list, or other public list.
- Customer has negative or contradictory publicity.

Red flags



Customer profile

- Customer makes inquiries about sum limits and other restrictions.
- Customer's profile is different from normal customer profiles.
- Customer operates during times that differ from expected behaviour.
- Customer has connections with high-risk jurisdictions, sanctioned countries and/or tax havens.
- Customer is a PEP who is influenced to carry out illicit activities.
- Customer is on a sanctions list.
- Customer has connections with organised crime.
- Customer has connections with other criminal activity.
- Customer uses a front man to remain anonymous or hide their identity.
- Customer requests documentation to an address other than his own.
- Customer has several different accounts, possibly held in different names.
- Customer has an unusual IP address.
- Customer doesn't confirm the actual beneficiary of transactions.
- Customer behaviour analysis indicates abnormality and makes no economic sense.

Transactions

- Customer often makes transactions close or below the thresholds.
- Transactions that could be linked to identity theft, a stolen account, or cybercrime
- Quick movements of funds to/from virtual currency platforms.
- There are many payers connected to one single payee without apparent purpose, or vice versa.
- Registration of a new customer and a large volume of transactions within a short period of time.
- Account is repeatedly credited and debited without apparent purpose.
- Transactions without apparent economic rationale or legal purpose.
- Deposit and withdrawal of funds and closing of the account within a short period of time.
- Unusually high amounts of transactions.
- Complex transactions.
- Circulation of funds.
- Use of bill payment services is exceptional in view of, e.g. the sums and purposes of use.
- Transactions from customers with different names and addresses are effected from the same IP address.
- Transactions do not meet the client's declared nature of business or declared usage of the service.
- The customer resides in one country but uses a foreign IP address without a reasonable explanation.
- Customer transfers funds to accounts to which donations are made by a number of other parties as well.
- Customer instructs all funds to be deposited into a third party's account.
- Domestic customers are using foreign accounts.
- Use of instant-buy services or making instant transfers with large sums.
- A large volume of withdrawals within a short period of time.
- Links to countries that present a high risk for money laundering and financing of terrorism.
- Links to safe havens/tax havens.
- Links to sanction lists, official freezing lists, or other public lists.
- Links to members of organised crime groups.
- Links to PEPs, particularly in foreign countries.
- Government officials or employees conduct disproportionate transactions.
- Transactions with links to non-profit organisations.
- Customer purchases goods or a combination of goods that could be used for terrorism.

The Black Wallet project is funded by the European Union's Internal Security Fund – Police. The content of this document represents the views of the author only and is his/her sole responsibility. The European Commission does not accept any responsibility for use that may be made of the information it contains.

POLIISI
KESKUSRIKOSPOLIISI
Centralkriminalpolisen
National Bureau of Investigation

Polisen
Swedish Police