Assignment
"*Transaction monitoring task*"

Candidate: Andrea Guarriero

Milan, 03/07/2024

Transactional Customer Risk Rating – Methodology & Caveats; possible future developments

A comprehensive approach

To perform a customer segmentation and assess risks from transactional behavior, we developed a **Customer Risk Rating "CRR"** framework.
We decided to adopt this kind of approach, in order to have a comprehensive evaluation of the behaviors of the customer base: to not overweight some of the risks while underweighting or even ignoring others, while segmenting the customers, and have in such way a comprehensive **Risk Based Approach** to the assignment.

The Framework is based on a number of KRIs, each reflecting a specific transactional risk of the business relationship with the customer.
For each KRI the customer receives a specific score/range of scores. The scores are then summed, and a Risk Segmentation is determined among "Low", "Medium-Low", "Medium-High", "High", reflecting the overall AML riskiness[1] of the business relationship.
The segmentation is meant **also** in a **prioritization logic** (Higher risk clients have to be scrutinized deeper and with higher accuracy) and a **resource allocation logic**[1].
The single KRIs are listed in the next slide, together with their rationale and technical fields used to elaborate them.

The CRR framework focusses on transactions and related risks (e.g. companies in *financial difficulties*, trying to wire sums outside of the bank; cross-border activity; so called Structuring&Smurfing).

Possible developments

Possible developments of the analysis could include adding to the dataset and using in the CRR some of the following data:
- **Customer data/ CDD[2] data** (e.g. legal form, date of birth "DOB", place of birth "POB", expected country of business, PEP status, UBOs): some transactional behaviors could be ordinary for some customers (e.g. frequent transactions for large corporations), while some risks are typical of other customers (e.g. customer with residence in High Risk Countries)
- **Date** data (e.g. date of transaction, would allow to identify transactions in high time proximity, or dormant accounts)
- **Business segmentation** (e.g. HNWI status)
- **Type** of transaction (e.g. cash deposit, check, credit card payment)

Caveats on data

!

During **data quality** checks we identified the following deviations, for which we suggest reaching out to data/process owners to understand a potential business logic:

- **CustomerID «0»**

Multiple transactions of a CustomerID 0 have been identified in the dataset (i.e. 19 for a total amount of 77.169€).
Since this could be a legacy of past M&A operations between previous banks, data migrations and since there are multiple transactions that look like they make business sense: we advised to **keep** them in the dataset, while waiting for a response from the data owner.

- Credit/Debit **negative values**

Multiple transactions have been identified in the dataset (i.e. 102 for a total amount of 53.115€), having negative amounts. Those transactions have both signs (Credit, Debit): we initially hypnotized a reimbursement logic, but the underlying business logic is unclear.
Since it is unclear to us if those transactions have a business sense, we advised to **exclude** them from the dataset.
We estimated a limited impact, since it appears only couple customers have more than 1 transaction of such type and the max amount of such transactions is less then 2.200€.

We decided to follow this approaches also considering the full dimension of the original dataset and its balance[3]:
- 10.000 customers
- 155.181 transactions for absolute amount of 779.024.847€

1. Risk segmentations reflects the expected behavior of the client, based on overall past behavior: e.g. a Low risk client is expected to engage in low risk behaviors on a stable basis and with a stable transactions pattern. In this way, the Banks can quantify the expected amounts of compliance resources to invest on different clients management;
2. Customer Due Diligence in its various forms (e.g. EDD – Enhanced Due Diligence);
3. The dataset looks fairly balanced: average amount of transactions is aprox. 5.020€ and median amount is 5.001€;
4. Some KRIs have been evaluated and excluded due to low significance in the given dataset (e.g. round amount transactions).

Transactional Customer Risk Rating – Methodology & KRIs for Assessing AML Risk

KRI	Rationale	Fields used*
Not Nordic Only transactions	Due to the high level of **integration** between **Nordic countries**, we consider them as a single country-market. Both because – following data exploration – (i) it appears to be a common pattern of the customer base to transact massively with a mix of the 3 countries (indicating **factual strong business ties** between said countries) and we partially expect such behavior from clients of a Nordic bank, (ii) because of the high level of cooperation between those EU countries (both in and outside the EU framework), strongly mitigating risks of cross-border transactions. We consider at higher risk clients transacting not only with Nordic countries (i.e. Finland, Denmark, Sweden).	**TransactionCountry**
Frequent transactions	High frequency could potentially hide **structuring**[1], and/or could facilitate hiding of high risk transactions in the multitude on low risk ones. Moreover, such activity probably is not mediated by a physical branch and the absence of a physically **onsite relationship manager** could reduce scrutiny and make more difficult to identify high risk transactions. We consider at higher risk clients transacting with higher frequency during the month (assumed as 20 workdays&4 weeks; 5 workdays weekly).	• **COUNT(TransactionCountry)** • **SUM(TransactionAmount)**
High Risk Countries	Transacting with High Risk Countries "HR" is a higher risk behavior, since – among other reasons – (i) money crossing borders could be more difficult to **track**/recover in the destination jurisdictions; (ii) **law enforcement** international cooperation could be hindered/reduced/ineffective; (iii) the **legal framework** could be deficient in prosecuting financial crime. For the purpose of this Assignment, only Romania has been considered HR. Cyprus, although it's *troubled* reputation, is not considered HR[2].	• **TransactionCountry** • And ratios between **TransactionCountry** components
Russia[3]	Although not formally classified as a High Risk Country[2], we consider transacting with Russia a higher risk behavior, due to (i) the current **geopolitical** situation (e.g. Conflict in Ukraine), (ii) the high **Financial Sanctions risk** and (iii) due to possible **weaponization** of international cooperation/lack of cooperation by the Russian State[4]. We expect customers still transacting with Russia to have very strong business rationale.	**TransactionCountry**
Outgoing and incoming amounts ratio anomalies	High amounts of outflows in relation to inflows could indicate a **company in financial distress**, trying to hide sums in advance of a bankruptcy or other legal proceedings. Outflows too similar to inflows could instead indicate a **shell company**, producing fake invoices for tax fraud/ evasion purposes. We consider such events at higher risk	• Ratio between **TransactionSign** components • **SUM(TransactionAmount)**
Many-to-One / One-to-Many Scheme	Highly "skewed" ratio between incoming transactions and outgoing transactions (and vice versa) could indicate so called ***smurfing*** (i.e. multiple customers performing a unitary transaction in pieces, in order to make more difficult following the so called *paper trail*). This is also possible if in a month there are no transactions of one type (e.g. a month with only Credit), to **evade Transaction Monitoring Tools rules**. We consider clients having a highly skewed relation between Credit and Debit (or the absence of one type of transactions) at higher risk	• Ratio between **TransactionSign** components • **COUNT(CustomerID)**
Unusual transactions	**Deviations** from usual/past behavior could indicate – among others – (i) the risk of use of the account by an **unauthorized third party**, in particular in case of use of remote accesses (e.g. by App/Internet), (ii) an attempt at **structuring** or disguising a high amount transaction. We consider the presence of unusual transactions a higher risk behavior	• **STDEVP(TransactionAmount)** • Average of **TransactionAmount**

1. Artificial fragmentation of a single transaction in multiple smaller ones, in order to avoid Transaction Monitoring detection rules and/or reporting thresholds;
2. According to FATF – Financial Action Task Force (the international body setting multiple standards for AML) publications on 23/02/2024;
3. In the current dataset only 1 customer has been identified transacting once with Russia for a sum below 1.000€;
4. Russian State proved to be willing to use its legal system with the purpose of damaging so called "*unfriendly countries*" in the West: by e.g. seizing assets of western companies, refusing to return leased planes, making unclear the legal protection and recognition of western judicial decisions for western banks (e.g. Gazprom vs UniCredit Russia, a case worth aprox. $480 mln).

* Only the fields have been listed.
For the comprehensive logics used, please refer to the techincal scripts shared.

Customer Segmentation & *Romania rule*

Threshold determination

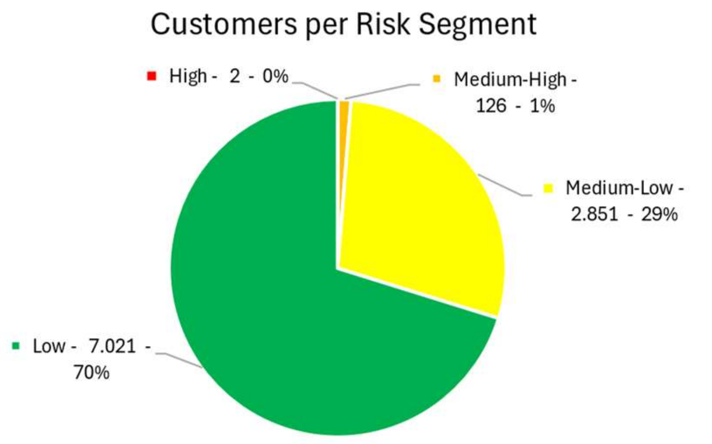
The value for rule "**Total Monthly Incoming transaction amount from Romania** > threshold_value" has been identified for the various Risk Segments as per the table in the bottom right corner.

Since the datapoints (customers and their monthly aggregated transactions) per segment looked acceptably balanced[1], we used the ***n sigma method*** (more on the method also on the next slide)[2] to identify the threshold.

Once the data has been checked for skewness, a standard deviation for each segment has been calculated[1].
For each segment, a *number* of sigma to use has been determined, **balancing** between the statistically stronger methodology in identifying outliers (i.e. 3 sigma) and a more **Risk Averse approach** by the Bank (0-1 sigma). The latter aimed to scrutinize a higher number of clients, while accepting a higher number of false positives.

The **final calculation** considered 2 sigma ("Medium-Low" segment) and 1,5 sigma ("Medium-High" segment), to reflect a lack of Risk Appetite and to scrutinize more customers with the growing riskiness of the business relationship.
Since only one client has been identified in the "High" segment, – on a Risk Based Approach – we determined that all High segment customers have to trigger alerts. There are currently no Low risk segment clients transacting with Romania.
Such approaches could be fine-tuned according to actual Risk Appetite Framework of the Bank.

According to the CRR framework is virtually impossible for a client transacting with the High Risk Countries to be in Low risk segment. Therefore, for the **Low Risk Segment,** it's currently **not possible to determine a data driven threshold** based on the available dataset, since we do not expect such event to happen at all. To prevent technical errors, it can be set to 0.
In a production environment, additional considerations should be made regarding the frequency of CRR, how transactions are managed by different IT applications, etc., in order to **balance sustainability** of the approach and of the risk management with granularity and depth of **scrutiny**.



In the chart above and in the table below we represented the **distribution** of the **customers** in the dataset for the various Risk Segments of **the Customer Risk Rating** implemented for this assignment.

The new **Romania** rule would be **triggered** by the following 6 customers.

It's interesting to note that in **mainly segmented** as **High or Medium-High** by the Customer Risk Rating framework, which could suggest an effective methodology in Customer Risk Rating.

CustomerID	Risk Segment	Transacted Amount
4473	High	21.439
2845	Medium-High	134.929
7082	Medium-High	18.530
2052	Medium-High	18.209
89	Medium-Low	12.865
3844	Medium-Low	15.919

Segment	# Customers	Threshold
High	2	0
Medium-High	126	15.044
Medium-Low	2.851	11.646
Low	7.021	- or 0[3]

1. An *average* and *median* amount of the aggregated transactions have been determined for each segment to check balance and skewness: the two values looked acceptably similar to determine acceptable balance. In the Medium-High Segment one of the datapoints was 134.929€, while no one of the 30 other was higher than 19.000€. We excluded said datapoint from the calculations, since it was strongly skewing the dataset;
2. Average + n standard deviations (more on the method on the following slide);
3. According to the CRR framework used for segmentation, it's virtually impossible for a client transacting with the High Risk Countries to be in Low risk segment. More on this in the current slide box.

Customer’s atypical behavior – ID list & methodology

Atypical behavior determination

We identified **8 Customer IDs**, which transactions seem to us **strongly deviating** from their typical behavior.
For all of them the rationale has been the same and it’s based on the following methodology.

A **typical behavior** has been identified for every customer, disaggregating for Credit and Debit transactions, and a threshold has been defined for each customer (average + 2 standard deviations[1]) : exceeding said threshold with a single transaction, indicates a deviation from typical behavior for said transaction.

The **single transactions** of all customers have been **ranked** based on the deviation from said customer’s behavior threshold.

The **top 25 transactions** – the most *deviating* from the threshold – and the related clients have been selected.
A table on the side summarizes the selected customers, their Risk Segment and the number of unusual transactions identified in the top 25 *deviating* transactions.

It is interesting to note that the extracted customers are **mainly segmented as High or Medium-High** by the Customer Risk Rating framework, which could suggest an effective methodology in **Customer Risk Rating**.

Customer ID	Risk Segment	Number of unusual transactions
5860	High	18
6741	Medium-High	1
2845	Medium-High	1
1519	Medium-High	1
570	Medium-High	1
6817	Medium-Low	1
6847	Medium-Low	1
4277	Medium-Low	1

The n sigma method approach

The so called *3 sigma method* is considered to be a statistically accurate method to detect **outliers**.
The 3 sigma method establishes that a datapoint beyond 3 standard deviations from an average is an outlier.
We applied a similar methodology: to be more Risk averse, we used a “***2 sigma method***”, in order to include more customers to scrutinize.

While the 3 sigma method stipulates that a ≈99,7% of datapoints will *not be* an outlier, a 2 sigma method should identify *only* ≈95% of datapoints as *not outliers*.
This **conservative approach** allows to identify more customers to scrutinize[2], while accepting the risk of a higher share of false positives (i.e. customers with transactions with no risk, even if unusual).

It has to be noted that this approach is based on **past behavior** of a client and, as such, does not account for potential explanatory data or logics (e.g. reason of the transaction, notes in the bank’s systems). This could potentially increase the share of false positives and have to be considered from a sustainability perspective.
It’s possible that the methodology used will need **fine tunings** or even a full methodology changes, to account for test results and reduce the false positives shares.

1. We used a variation of the so called *3 sigma method,* adjusted to 2 sigma to reflect a lack of Risk Appetite (similarly to what has been done for the Romania rule);
2. An increased number of scrutinized customers could also be a strong argument to defend a Risk Management model in a discussion with the Regulators.