Why it's a bad idea to recycle your name screening solution for transactions

Fintechs need to step up their game and use adequate technology to screen their payment transactions.

For many Fintechs, compliance with financial crime regulations is an iterative and painful discovery journey. While banks have been increasingly exposed to these regulations for over two decades, most Fintechs only got created over the last few years and their initial focus was – rightfully– on offering a distinctively better customer service and experience.

From a financial crime compliance perspective, their initial priority is often to be compliant with Know-Your-Customer (KYC) regulations. This leads to the setup of an appropriate watchlist screening solution for customers' onboarding and their ongoing monitoring.

At a later stage of development, the Fintech faces the need to also screen customers' transactions against sanctions and embargos. The tempting tactical choice is then to leverage the existing KYC screening solution: extract the sender and receiver names from the payment instruction and screen them like during onboarding.

However, this deceptively simple approach to transaction screening creates a huge regulatory risk, increases customer friction and leads to significant operational costs.

KYC Screening and Payment screening: different purposes and modus operandi

KYC screening solutions and payment screening solutions are serving separate purposes and operate differently:

- **KYC Screening** (also called 'name screening') is used at the time of customer onboarding and for the continuous monitoring of the customer databases. These solutions help identify a variety of risks by checking names against three types of lists: (1) Sanctions lists (for embargos and counter-terrorism financing), (2) Politically Exposed Persons (who represent a different category of risk) and (3) adverse media (e.g. bribery, corruption, environmental, social or organisational risks). The watchlists used for KYC screening are huge, containing several millions of entries, and constantly growing. However, the technical performance (i.e. throughput) of KYC screening solutions is a secondary consideration, as most of the continuous monitoring happens in batch.

- **Transaction screening** solutions are mission critical. They are checking transactions (for example payments) in real-time while they are processed, and any alert can create execution delays for the customer. These solutions need to detect possible risks in any data point of the transactions: sender, receiver, ultimate beneficiary, intermediaries, payment instructions… with many of these fields being not structured and containing free text. The goal of transaction screening is to identify possible risks in terms of sanctions, embargos and counter-terrorism financing, with PEPs and adverse media being out of scope. As such, the watchlists used are much smaller, typically in the range of tens of thousands of entries.

The one-size-fits-all approach simply does not work

Trying to use a KYC screening solution to also screen transactions creates three major issues:

- **Customer friction and operational costs**. KYC screening solutions screen against much larger watchlists, including items which are not relevant in the context of transaction screening, like PEP or Adverse Media. Instead of screening against watchlists of a few dozen thousand names, screening happens against watchlists of millions of entries. This results in an unnecessary large number of false positives and irrelevant hits. As every alert on a payment puts it on hold, many transactions end up being delayed, to the frustration of the end-customers.
- **Regulatory risk**. The structure of a payment instruction is very different from a customer record. By just screening the sender or the receiver of the payment, a lot of essential information is ignored, creating a very significant regulatory risk. The classical example is the 'purpose of payment' or 'sender instructions' fields – typically a free-format text (imagine instructions stating: "Shipment of container to Tehran"). Another example would be the banks involved in the transactions (e.g. the receiver's bank or intermediary banks), which are usually not represented by their names but by their BIC codes. Screening these fields call for specific techniques such as entity resolution or BIC expansion, that are not part of KYC screening solutions. The issue goes beyond the regulatory risk that Fintechs create for themselves: these shortcomings in payment screening will cascade risk to the correspondent banks that are often involved in such payments. These correspondent banks expect their Fintech counterparts to properly screen their payments and would otherwise simply refuse continuing to process their payments.
- **Low performance**. Transaction screening solutions are deeply optimised for high throughput and low latency. Using a KYC screening solution for payments will result in significantly lower performance, if only because of unnecessarily screening against the much bigger KYC watchlists. Issues with throughput and latency can have serious consequences in use cases like instant payments, where every millisecond counts and SLAs between correspondents are very strict.

The right approach to payment screening

For Fintechs aiming to step up their game in financial crime compliance while delivering a great customers' experience, using an adequate and dedicated transaction screening solution is undoubtedly the only way forward.

Latest transaction screening solutions offer standardised cloud-based APIs allowing for easy integration with Fintechs' technical architecture. This approach provides excellent performance and efficiency while leaving the Fintech totally in control of the end-user experience.

API-based payment screening solutions can also help improve the customer experience at the time of payments initiation. Since they are integrated directly in web or mobile applications, screening can actually happen in real-time while the customer is in the process of initiating their payment. The outcome of this screening can then be used to dynamically adapt the user flow directly in the app, either by asking for more information or to manage customer expectations (e.g. there is no point in suggesting an 'instant payment' option if the pre-check shows a sanctions hit that will hold the transaction pending investigation).

Adopting a real payment screening solution not only reduces the regulatory risk but also allows for a better and more controlled customer experience: definitely a no regret move for Fintechs!

Contact Us

info@neterium.io
linkedin.com/company/Neterium
@neterium