



Banking-as-a-Service and Financial Crime Compliance

Banking-as-a-Service and Financial Crime Compliance

Six key criteria for selecting a watchlist screening solution for BaaS providers

Banking-as-a-Service (BaaS) is on the rise. An increasing number of non-bank players (e.g., e-commerce platforms, retailers) are now embedding financial services such as payments, *Buy Now Pay Later*, wallets or lending in their offering to further improve their customer experience and maximise the value they can capture. And it does not stop there: some banks are also increasingly interested in using BaaS as they see an opportunity to focus on what they do best and leverage other players to provide part of their offerings in areas where they lack either the scale or skills to efficiently develop themselves.

The race has therefore started on the provider side to create attractive BaaS offerings. Some traditional banks see a new opportunity to leverage their scale and address the expected decline in their existing revenue streams by developing a new market activity. Beyond banks, a series of new Fintechs focusing exclusively on BaaS services have also emerged over the last few years. More recently, large established Fintechs (such as Stripe) also jumped in, as they see BaaS as an immediate adjacency to their already successful business model.

Financial crime compliance is often a component that BaaS providers aim to provide as part of their offering.

The scope of the services offered by BaaS providers can differ widely, ranging from a narrow focus on a specific service (e.g., card issuing, *Buy Now Pay Later*) to a full-fledged universal banking platform. Some are only offering a pure technology play while others also include some Business Process Outsourcing as part of their offerings. The choice is now very large, and the number of BaaS providers is expected to further grow in the quarters to come.

Financial crime compliance is often a component that BaaS providers aim to provide as part of their offering. One of the key financial crime compliance aspects to address is watchlist screening, both in a KYC context, for the screening of clients (e.g., for client onboarding and monitoring) as well as for the screening of transactions (e.g., payments) against sanctions and embargos.

This paper highlights the [6 key criteria](#) that BaaS providers should look at when selecting a watchlist screening technology to integrate in their BaaS offering



Banking-as-a-Service and Financial Crime Compliance

1 - Effectiveness: the license to play

It may seem obvious but the most important criterion for selecting a watchlist screening technology is to make sure it is effective at doing the job, i.e. effectively identifying the clients that should be reviewed in depth and preventing transactions with sanctioned entities or individuals.

Easier said than done though, as regulators' expectations go far beyond the so-called "perfect" matches and include among others:

- *Advanced fuzzy logic features* (e.g., abbreviations, spelling mistakes, name/first name inversions, patronyms, synonyms, titles, split/merged words, missing/added letters);
- *Screening of different alphabets* (e.g., Cyrillic, Chinese, Arabic...);
- *Advanced transliteration capabilities* (to compare different character sets to watchlist items that are often provided in Latin characters);
- *Detection in unstructured transactions data.*

A watchlist screening provider unable to provide demonstrable effectiveness is a non-starter, as it would reflect badly on the whole BaaS offering.

2 - Architectural fit

BaaS providers have specific and demanding needs that require a modern, secure and future-proof architecture. The following are key features that the Watchlist screening technology provider should offer:

- a) *API-native and Cloud-native* to allow for an easy integration, automatic maintenance, cost efficiency and scalability.
- b) *White-labelled engine*. For the platforms built on BaaS, providing a smooth and frictionless customer experience is key. Since this requires tight integration into their processes, BaaS providers should look for a watchlist screening provider who can offer just the screening engine as a component, detached from other tools such as alert management, orchestration, mapping... that are often bundled with solutions.
- c) *Multi-tenancy* to ensure the BaaS provider can accommodate each client's specific needs (watchlists to be used, risk policies, etc) while serving them from one single infrastructure.
- d) *Security by design*. BaaS clients will expect the highest level of security, often demonstrated through certifications such as ISO27001 or SOC2. BaaS Providers should in turn expect such a high level of security from their watchlist screening provider.



Banking-as-a-Service and Financial Crime Compliance

3 - Technical performance

The use cases addressed through BaaS can be extremely demanding and the watchlist screening technology provider should offer state-of-the-art technical performance to ensure it does not create a bottleneck in the BaaS processing capabilities. The dimensions to watch for here are:

- a) **Throughput.** BaaS providers will process huge amounts of simultaneous transactions and on-boarding checks, often with peak periods. Each BaaS provider will have their own throughput requirements, but a future-proof system should offer a throughput in the excess of 50,000 screening requests per second.
- b) **Latency.** Beyond throughput, low latency is key to address use cases such as instant payments. To address all their clients' use cases, BaaS providers should make sure their screening component has an average latency below 25 milliseconds.
- c) **Availability.** Finally, service availability has become essential and 24/7/365 is the new norm, especially for global BaaS players. Gone is the time where *Allowed Downtime Windows* were acceptable. The Watchlist screening provider should be always on, even during software and watchlist updates. Transparency on this dimension is expected, with several watchlist screening providers already publicly publishing their availability figures.

4 - Flexibility and Efficiency

Financial crime compliance is all about balancing effectiveness (i.e., the regulatory obligation) and efficiency (i.e., the number of false alerts raised as a negative side effect of an effectiveness objective).

BaaS providers should make sure the selected watchlist screening technology offers:

- a) **State-of-the-art efficiency out-of-the-box.** Each false alert needs to be analysed manually and creates painful friction in the user experience by delaying payments or denying authorization. Therefore, achieving the lowest possible level of false alerts is essential, but fine-tuning a screening engine is not the speciality of a BaaS provider, so the engine needs to provide with an acceptable level of false alerts right out of the box, without requiring any specific configuration.
- b) **Flexibility.** While some BaaS clients will be happy to apply the optimised out-of-the-box settings of the screening engine, one should expect that most clients (banks definitely) will want to adapt their screening parameters (e.g., lists to screen against, alert threshold, screening policies) based on their own risk appetite. Beyond the flexibility in parameter selection and given the increasing complexity of the watchlist screening context, offering the ability to select and combine various watchlists from different watchlist data providers will certainly be an additional asset to address the needs of the most demanding bank and non-bank clients.



Banking-as-a-Service and Financial Crime Compliance

5 - Explainability

First-generation watchlist screening solutions used to operate as pure black boxes: a transaction or client name would raise a hit with little clue for an operator to understand the logic behind triggering a hit.

BaaS providers should seek to work with watchlist screening providers that offer full explainability of why alerts are (or -as important- are not) raised, for two reasons:

- a) **Regulatory expectations.** Regulated platforms built on BaaS need to be able to explain the functioning and logic of their watchlist screening solution to their regulators. The ability to fully understand and explain why an alert is or is not raised is a must for these clients.
- b) **Reducing support load.** If the screening solution is not providing the alert rationale, BaaS clients will undoubtedly reach out to the BaaS provider's support centres, resulting in lower customer satisfaction and high support costs.

6 - Data Analytics

BaaS providers will aim to leverage all data available, both to monitor their clients' usage as well as to use it to improve their services and unlock new business opportunities. The Watchlist screening provider should therefore provide much more than a simple 'hit/no hit' information and provide deeper analytics such as:

- a) **Consumption and usage patterns statistics.** This will allow BaaS providers to better understand how their service is actually being used by each of their clients (e.g., which kinds of transactions/customer records are triggering the most hits, which lists are the most used, etc). Based on these insights, they will be able to better help their clients optimize their processes or identify new business opportunities.
- b) **Data quality Analysis.** With modern screening engines, higher quality data always results in higher efficiency (i.e., fewer false alerts). The watchlist screening provider should therefore be able to identify or - even better - quantify data improvement opportunities in the client/transaction flows sent by each client (e.g., adding date of birth or location information).
- c) **Content resolution.** The resolution of content found in unstructured transactions (think of information related to ports or cities) will allow for powerful visualisation and faster decision making for analysts reviewing the alerts.
- d) **Context data.** Finally, the more information the screening engine returns (e.g., correlations in watchlist elements, resolved content, geo-coordinates) the more it allows the BaaS providers to correlate these data points, enrich their machine learning models and have a better value proposition.

Banking-as-a-Service and Financial Crime Compliance

Conclusion




BaaS is about offering state-of-the-art banking platforms or components to banks and non-bank players, that can be combined and embedded in customer journeys to offer a truly distinctive end-customer experience.

Financial crime compliance is a necessary piece in the BaaS puzzle and - when done right - can be turned into a competitive advantage.

Financial crime compliance is a necessary piece in the BaaS puzzle and - when done right - can be turned into a competitive advantage. Selecting an advanced watchlist screening technology provider which can

adapt to the specific requirements of BaaS environments is essential to fulfil the vision of frictionless customer experience.

Contact us

 info@neterium.io
 [linkedin.com/company/Neterium](https://www.linkedin.com/company/Neterium)
 [@neterium](https://twitter.com/neterium)