en.SafeWatch Filtering elevates the compliance debate, evolving into an Expert System that further reduces cost of compliance, increases security, and paves the way to the future in Embargo and Sanction Filtering

The capability to replay previous decisions, which has been recently added to en.SafeWatch Filtering, enables the automatic release of transactions similar to those previously released by operators. It also helps prevent operators from releasing a transaction similar to a previously blocked one. In today's fast evolving payments landscape, Expert System assistance has become a definite prerequisite to filtering Instant Payments.

The need for a comprehensive and reliable sanction screening program for every Financial Institution has become more critical and more apparent as a result of the ever-changing regulations and the highly publicized fines that have hit many Financial Institutions in the past few years, causing significant financial losses and reputational damages.

en.SafeWatch Filtering features a state-of-the-art filtering engine that implements both public and proprietary algorithms that apply fuzzy logic to match suspected patterns in messages and in customer names with entities blacklisted by authorities such as OFAC, EU or UN. Many blacklisted entities also carry low quality aliases, which complicate and increase the effort required by Financial Institutions to clear the false positive hits generated by the filtering software.

Over the past decades, EastNets has worked closely with Financial Institutions of all sizes on a global scale to understand the daily operational effects of compliance issues, and it has developed solutions that reflect this experience, resulting in further improvements in en.SafeWatch Filtering.

A. ADDITIONAL COST REDUCTIONS

So far, en.SafeWatch Filtering has offered affordable compliance to Financial Institutions by delivering the lowest possible rate of false positive hits in filtering customer names and transactions (SWIFT, SEPA or other domestic payments).

This has been achieved mainly through two mainstays of its range of functions, namely Good Guys and Violation Filters:

- A Good Guy can be unconditional (e.g. "General Montgomery" is Good Guy against the alias "General" of Charles BLE GOUDE on the OFAC SDN list) or built with a wide variety of conditions, such as the degree of similarity between the scanned text and the blacklisted entity, or the SWIFT message field where the match has occurred.
- A Violation Filter is a rule that qualifies when a given List should apply. For instance, Compliance Officers may decide that the UK HMT list should only be applicable to payments in GBP or to messages sent to Financial Institutions residing in the UK.

Under the current filtering process, operators frequently release SWIFT payments stopped because the ordering customer or the beneficiary unfortunately has a blacklisted element (e.g. «Hassan», «Abdullah», «BENTLEY») as part of their name. This creates a tremendous waste of time and effort, and therefore of money.

On the one hand, the new Replay Decision module now "remembers" the exact cases (e.g. the account number and full name of the customer) where Violations have been released by operators (1, 2 or 3, as per configuration) by recording in a dedicated database table all occurrences of filtered string, matching blacklisted entities and other essential context elements. Should a new occurrence of the same pattern reappear, en.SafeWatch Filtering will automatically identify the pattern and reapply -"Replay" - the previously taken decision.

Thanks to this feature, en.SafeWatch Filtering has become an increasingly autonomous expert system, and rates of violations being handled automatically can reach significant levels just a few months after activation of the Replay Decision feature.

On the other hand, the new Enhanced SWIFT Format module becomes fully aware of the structured fields 50F and 59F of a SWIFT payment, and prevents, for instance, any hit of an address subfield (i.e. starting with "2/") against a blacklisted entity linked to an Individual or Group.

B. ADDITIONAL SECURITY

Whilst false positive violations generate tremendous costs, real violations (i.e. hits where the name being filtered proves to be the blacklisted entity itself) create high risks. Indeed, whilst operators release on average over 99% of the transactions stopped by the filter, the risk of human error (i.e. releasing a true hit inadvertently) is very high.

en.SafeWatch Filtering now assists you in mitigating those risks in two ways:

- Firstly, the new Replay Decision module also stores the context of all Real Violations. It then prevents the same or another operator from releasing a new message whose context is identical to that of a message previously stopped, by displaying a pop-up alert, advising the user, as a protective step, to consider the decision to release a message which is very similar to a previously blocked one.

- Secondly, the new Automatic Block module prevents an operator from releasing a 100% hit against specific, usually private, blacklists containing unique identifications of sanctioned or embargoed entities, such as Mule Accounts, Vessel or Aircraft registration numbers, or Chinese Commercial Codes.

Another significant compliance risk consists of back-office operators or customers resubmitting a previously blocked transaction after removing the suspicious content. The en.SafeWatch Filtering Stripping Detector module enables your Financial Institution to set up its own criteria of similarity between two MT103 or MT202, such as amount, currency, ordering or beneficiary customers' names, so that a potentially stripped message will be stopped by the filter even if the suspicious information is no longer present.

FATF Recommendation 16 addresses the fundamental issue of data quality related to the originator of a payment, as well as the beneficiary, for both sent and received transactions throughout the payment chain.
The new functionality allows Financial Institutions to monitor wire transfers, including SWIFT MT103, MT202 COV, MT205 COV, as well as SEPA messages, and easily detect missing information including insufficient originator and/or beneficiary information, and hold message processing until a decision is taken on its completeness and adherence to the new requirements.

C. KEY TO THE FUTURE OF INSTANT PAYMENTS

Automatic replay of previous decisions is also required when an ultra-fast reaction time is necessary. With a total of less than 10 seconds for the complete execution of an instant payment, the standard filtering process involving decisions made by operators has become obsolete. The Replay Decision module can be tailored to offer additional flexibility in this context, with slightly less stringent operational rules as for SWIFT traffic, for instance by enabling the repetition of a decision after release of a payment having the same context by just 1 operator.

ABOUT EASTNETS

EastNets® is a leading global provider of compliance and payments and cloud solutions for the Financial Services industry. Over the past 30 years EastNets has built distinctive expertise to develop and implement standardized and individual solutions against financial crime, and for risk management, monitoring, analysis, reporting, and state-of-the-art consultancy and customer support. Over 1000 customers including some of the largest international Financial Institutions rely on EastNets solutions and professional services, and over 300 corporate and Financial Institutions rely on EastNets for outsourced SWIFT connectivity and compliance software solutions made available as a service through its fully managed service bureaus.

EastNets is a global company with regional offices in major cities, supported by a large network of global strategic partners.

CONTACT US

info@eastnets.com
www.eastnets.com

EastNets®
en.abling confidentiality