Introduction

The processing of duplicate and fraudulent messages is easily avoided and yet it occurs far too often. Increasingly, organisations have invested in sophisticated automation that can process large volumes of requests in real time. These companies need to protect themselves against the financial and reputational risk attached with processing duplicate and fraudulent payments.

Aqua Global's Duplicate Message and Fraud Detection Module safeguards an organisation from this problem arising as a result of accidental or deliberate actions.

Duplicate Detection

Many institutions have interfaces that accept messages from many different channels. Mistakes can occur such as a channel releasing a duplicate set of transactions that could be automatically processed within a few seconds, including the creation of outward settlement transactions. Alternatively, a manual customer instruction could inadvertently be processed more than once. Duplicate detection operates in real time, automatically highlighting potential issues for all inward and outward message channels by proactive alerts and moving these messages to a repair/exceptions queue for review prior to processing or transmission.

Fraud Prevention

The threat of cyber-attacks is ever increasing and it is of paramount importance to ensure the integrity of every transaction processed and increase barriers against fraud. Once access is achieved, attackers can operate silently for extended periods of time learning patterns. They will create new "payment corridors" based on combinations of target and beneficiary banks, often choosing to blend fraudulent transactions with legitimate traffic during busy periods in the day. For institutions that have invested in automation, this is a real threat. The solution provides the ability to control and monitor all messages that, for example, are sent to identical beneficiaries over a specified time period. This will help detect transactions that potentially make up a money laundering scenario or instructions that have been injected from an external attack to transfer funds illegally.

The solution is highly flexible and can be configured to select exactly, what data elements in a message are to be used, to determine if a message is a duplicate or fraudulent. The solution can be configured for any service channel such as SWIFT FIN, ISO 20022, Local Clearing, mobile banking etc. as well as manual input.

Benefits

- Monitors and protects in real time
- Increases security and reduces risk
- Simple to use
- Quick to deploy
- Highly scalable for any service channel
- Automatic alerts for exceptions
- Minimal changes to existing environment
- Full audit