Know Your Customer (KYC) Executive Overview
with Know Your Vendor (KYV) and Know Your Employee (KYE)

Purpose
The goal of this whitepaper is to review the business drivers that are creating increased focus on the KYC issue, layout the major steps of the process, and educate the reader on ways that the Quavo/Pega solution can provide value. The same solution can be leveraged for KYV and KYE, creating a single investigative platform for knowing your customers, vendors and employees.

Background
FATF treaties with anti-money laundering and terrorist financing regulations are driving investments in the three major parts of an AML program:

1. Transaction Monitoring
2. Screening or List Processing
3. KYC investigations

Risk rating is interwoven to all three.

Transaction Monitoring software looks for out-of-pattern transaction behavior, or risky transaction behavior. It is normally implemented as a captive system, where nightly feeds of customer transactions are copied into a separate data warehouse. This database can get quite large, as up to 5 years of customer transactions can accumulate. Each night, a set of routines is run to look for abnormalities. Large cash transactions are typically reported to the bank's regulator. Suspicious transaction behaviors are reported, and are treated quite seriously. These "events" may also trigger a KYC investigation. There are companies like NICE Actimize that are dedicated to this problem.

Screening or list processing is the act of comparing all the customers in a bank against a set of "bad or risky" lists of people and companies globally, and can get quite complex. In compliance lingo, companies are referred to as legal entities, and there is a movement to create global unique identifiers (LEI – Legal Entity Identifier) for them. It can be very hard to accurately match a customer of a bank against some of these lists, and this leads to many false positives that (normally) humans need to resolve. There is also a delta delta challenge. Initially, all the bank's customers are compared to all the lists, and any hits are evaluated for increased risk. But the next day, customers are added and deleted from the banks database, and names are added or deleted from the lists. So the new customers are compared to all the new lists, and the old customers are compared to the deltas of the new lists. There are companies dedicated to creating and maintaining these lists, and to provide the matching algorithms to decrease false positives. Bridger, World-Check, FircoSoft and Nomino Data are examples.

KYC investigations assess customer risk and must be performed without exception. There are two types of customers – individuals (humans) and legal entities (companies, trusts, FIs, etc.) Initially, KYC is done when a customer first applies for an account at the bank. Each subsequent time the same customer adds an account, the KYC needs to be re-performed. KYC investigations can also be triggered by events. An event may be a suspicious behavior hit from the transaction monitoring system. An event may be a list hit from new "negative news" about that customer, or even a maintenance change like a new address. KYC investigations can be triggered by periodic review cycles, which are set up by customer risk

or type. Normally, for complex customers, a KYC review is performed every 1 or 2 years. And finally, at any point in time for any reason at all, a manual KYC can be started.

KYC varies in complexity and scope depending on the customer type. Local individual customer KYC may just be the collection of identification, and a call out to a screening processor (bad guy lists). If there is no hit, then this type of customer KYC can be instantaneous. On the other end of the scale, large multinational corporate entities may take 2 to 3 months in the KYC process. There are now vendors that offer pre-packaged research for complex entities, thus saving work for each individual bank (i.e. KYC.com). In the middle would be wealthy individuals from foreign countries, and local businesses.

The type of KYC investigation that is performed varies substantially by customer type, customer risk, jurisdiction and regulatory law. For example, a bank in Brazil may have specific regulatory requirement for that jurisdiction issued by that country's regulator. If a bank complies with FATCA, then it would need to gather specific information for that law. If the customer was high risk because of a PEP (Politically exposed person) list hit, then the bank would need to perform enhanced due diligence. If a customer was opening a trading account in Paris, then the bank would need to conform to MiFID regulations. If the customer was a business, then the bank would need to gather corporate documents and understand the beneficial owners. Thus, the KYC questions and documents gathered to support the answers vary with each specific customer situation.

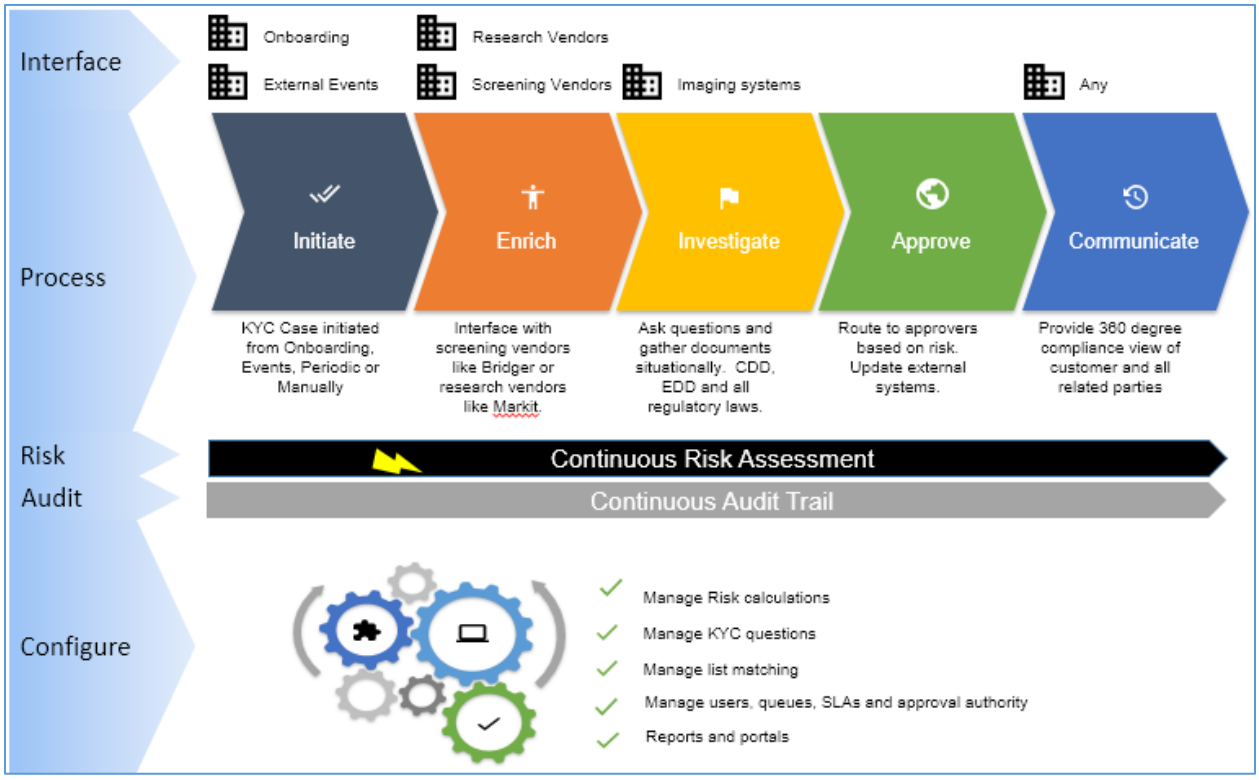
Customer risk rating is foundational to AML. Any data collected about a customer, their products, any hits from screening (lists), KYC questions, and related parties can be used to assess risk. Risk rating is normally low, medium and high. If risk is higher, the sensitivity of the transaction monitoring will be turned up and the KYC investigation will be more detailed (EDD – Enhanced Due Diligence) and periodic reviews more frequent.

Solution Vision

The Quavo KYC (QKYC) solution is a full end to end KYC process for all customer types for all regions, includes interfaces to existing systems and major external vendors, and can be utilized for KYV and KYE. The offering leverages the Pega KYC application which is built on the Pega platform (Pega 7) to create a full end to end solution aimed at local and regional Financial Institutions.

KYC is one part of an overall AML program. Normally, the bank will have implemented a transaction monitoring system from one of the many vendors who specialize in this area. Likewise, banks have been required to do screening for years, and have entered into agreements with various companies like Bridger or World-Check to provide these services. The QKYC solution leverages these companies' API's to call these services and use the resulting information to drive the KYC process.

.



Initiation of the KYC case can occur in four ways. Automatic interfaces from the onboarding system(s) create KYC cases. Likewise, specific events from other systems (external list processors, core banking systems, transaction monitoring) can create KYC event driven cases. The KYC application itself automatically creates periodic review KYC cases, depending on risk factors, customer type, etc. It also creates automatic cases to replace stale documents in a KYC file. And at any time a manual individual KYC case or a manual entity KYC case can be started. An API is exposed for other systems to create KYC cases, or the KYC system can reach into external systems and create KYC cases proactively.

Once the initial KYC case is created, the data is enriched mainly thru automatic interfaces to screening or list processing companies. API's from World-Check are included in PegaKYC, but typically each bank would have their own vendors, which would be integrated as part of the implementation. A Markit integration is provided for Entity background data. For most smaller banks, the KYC application will call out to the selected list processing vendor, and then use the resulting data as part of the case data and risk assessment. For large organizations, some screening operations can occur before the KYC case is initiated, leaving KYC to focus on high risk customers and complex customer types.

Investigations are driven by the KYC application and are situationally reactive based on customer type, customer risk, jurisdiction and regulatory law. The KYC application is delivered with over 45 types of KYC questions. These "KYC Types" are then applied to the specific situation. The core KYC types are Individual CDD, Individual EDD, Entity CDD and Entity EDD. Other KYC Types are specific to product, local jurisdiction and regulatory laws. Each KYC Type has specific questions and document gathering facilities. DLA Pieper, the world's largest law firm, created these KYC questions and KYC types from applicable law and best practices. For an additional charge, quarterly DLA updates can be purchased

from Pega. The bank can use these OOB KYC Types and questions, modify them to suit their needs, or create their own. Example KYV and KYE KYC types are provided as well. Any documents that need to be collected are attached to the KYC case with a pointer to the document repository (varies per bank).

The first time a customer is KYC reviewed, a master KYC profile is created. This includes related parties, which can be added to the investigation at any point in time and are spun off as related KYC cases. There are no limits on the number and depth of related parties, other than the investigations of these related parties needs to be completed before the final approval for the original customer can be given. Related parties that are not customers can be stored herein. When the customer needs to be KYC reviewed again, the information from the KYC profile is reused, allowing only differences to be investigated. This creates an opportunity for massive time savings, and allows for complete auditability of that customers KYC activities life to date.

The KYC case needs the proper approvals, again based on a user controlled configurations that we will set up based on the policies of the bank. A set of work queues and business rules are set up to drive these approvals. Some KYC cases can be automatically approved with business rules. Others may need to go to a Branch Manager for approval, or head of compliance for approval. Others will need more enhanced investigations and/or management approvals.

Once approved or rejected, other systems will need to be communicated to. For example, the onboarding system, if that was the origin of the case, will be electronically notified such that the customer and accounts can become transactional. Additionally, internal approvals can be executed on mobile devices, if appropriate.

A full 360 degree KYC profile view of the customer is provided and is the one source of truth for central KYC files. All KYC activity for that customer, links to related parties with a graphical representation, full risk profiles and detailed reporting is provided. A technique called Mashup can expose details of a customer's KYC case to the internet or mobile sites. This is particularly helpful to customers who are in the KYC process so they can access the status of their case and download required documents to accelerate KYC investigation time. Auto-generated email can also be used to communicate directly with the customer to gather necessary documents, or to update documents that will become stale.

The risk rating engine evaluates risk based on any data in the KYC case, or accessible from the KYC case. When data is gathered or changed, the risk is also recalculated in real time. If the risk increases, then the KYC application reconfigures itself and forces a more rigorous investigation and approval process. A default risk rating is provided for both individuals and entities using a Scorecard metaphor. A Scorecard is a business rule that is provided by Pega and configured to calculate KYC risk in this application. Risk rating operates on three types of data. Static data about the individual (length of time a customer, country of birth, country of domicile, occupation, etc.) or entity (length of time a customer, type of business, countries of operation, etc.) is combined with product risk based on that customer's portfolio, and answers from KYC questions. Related party risk is rolled up into the risk calculation of the primary KYC customer if desired. This risk rating is available thru an API, allowing other systems can access the risk rating of a customer.

It is essential that core behavior of the KYC application can be configured by nontechnical application administrators. Users must have control of their system. Using specialized wizards, a system

administration portal is provided to control the configurations. There is full security around the access of this portal, and full auditability of all changes made to settings within this portal. Essential configuration areas include risk rating, KYC questions, defining match probabilities, drop down tables, maintaining users, queues and SLAs, and reporting.

Way Forward

The Quavo KYC solution is built on Pega7 and Pega KYC, providing a fixed price implementation of a best in class, end-to-end KYC application customized to your needs and specific IT environment. The Quavo KYC implementation team are experts in KYC, participated in the design and development of the Pega KYC application, and have years of experience successfully implementing Pega projects. We look forward to understanding your needs and how best we can help you realize your KYC vision.