sanctions.

peace of mind

kyc.
monitor

❝

With the ever-increasing regulatory emphasis on organisations to actively demonstrate competent Anti-Money Laundering (AML) procedures and prevention techniques, it is a significant challenge for organisations to remain consistent in compliance.

AML compliance is critical …but it doesn't have to be difficult.

With the ever-increasing regulatory emphasis on organisations to actively demonstrate competent Anti-Money Laundering (AML) procedures and prevention techniques, it is a significant challenge for organisations to remain consistent in compliance. The penalties for those failing to meet cross border and national legislative requirements are becoming ever more severe, thus no organisation can afford to be without the correct tools and procedures.

A cornerstone to compliance is "Know Your Customer "(KYC). To be effective, this has to be more than just checking and managing customer documentation. It needs to include the ability to identify any unusual account activity that may be indicative of money laundering or fraud and understand the risk profile of each client.

Our solution

kyc.monitor is a sophisticated case management system that enables organisations to supplement their policies and procedures, improve their internal disciplines and provide clear evidence to the relevant authorities that effective and sufficiently robust AML controls are in place. Rigorous tools are in place to identify, review, document and report all suspicious activity.

It can be integrated seamlessly with other systems including cor financial's own products: sanctions.monitor (Watch-list checking), paragon (US fixed income portfolio accounting) and abraxsys (Core banking).

❝❝

Many organisations have manual or report-based systems to detect suspicious activity already; why should they consider a case management system?

SPEED: Report-based systems require a huge manual effort in the detections of suspicious activity and reports will become burdensome as volumes grow.

CONSISTENCY: Determination of what is and is not suspicious is open to the reviewer's interpretation.

COORDINATION: The reviewer will typically need to access other data sources to investigate a potential incident.

ACCOUNTABILITY: A report-based system has no integrated method to document any suspicious activity or demonstrate due diligence.

Key features

- Workflow based customer due diligence and monitoring.

- Suspicious activity is automatically detected based upon consistent rules.

- Rules are user definable and take into account different customer profiles.

- Users are focused on investigating, rather than looking for, suspicious activity.

- Fully audited details of the initial detection and subsequent investigation.

- Regulators and auditors are able to review the history of all aspects of an issue in a single system.

Case managment vs report-based systems

When evaluating a case management system against a report-based system, consider the following:
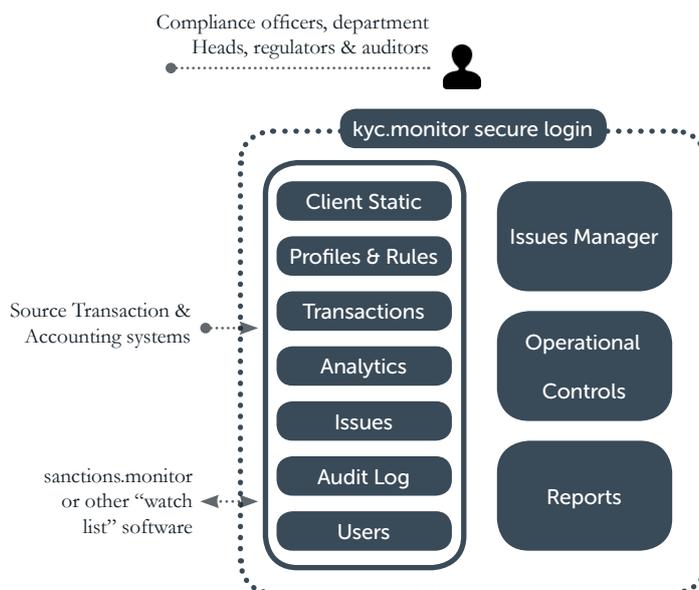
- Is it possible to use different criteria for different individuals and entities?

- How do you view all current and historic suspicious activity for a specific customer?

- Can you prove that a report has actually been checked?

- How frequently has a customer appeared on specific AML reports?

- Is the customer's risk class taken into account as part of the suspicious activity detection?

- How is the investigation recorded and retained for each suspicious activity incident?

- Can you monitor more stringently customers who have previous confirmed suspicious activity?

- How do you demonstrate to auditors and examiners the details of your investigations into each suspicious activity incident?

- When your business grows, what increased resources and effort will be required to carry out the necessary monitoring to enable you to remain compliant?

- Are cases of suspicious activity detected consistently and systematically?

❝

KYC monitor answers all of these questions and more by automatically detecting suspicious activity across the customer base from all business classes using configurable profiles and rules. Profiles are created to detect variations from expected behaviour for a customer or customer type. Each rule is designed to detect specific fraud and money laundering scenarios and can be configured to act differently depending upon certain attributes such as the customer type or customer's risk classification. Any instance of suspicious activity is elevated as an "issue" that contains all of the relevant details required.

fig.1 solution overview

Compliance officers, department Heads, regulators & auditors

kyc.monitor secure login

Client Static
Profiles & Rules
Transactions
Analytics
Issues
Audit Log
Users

Issues Manager
Operational Controls
Reports

Source Transaction & Accounting systems

sanctions.monitor or other "watch list" software

Customer due dilligence (CDD)

kyc.monitor provides a comprehensive solution to manage the customer account opening and account maintenance process which is a key part of any AML procedure. It maintains compliance details for each Person, Entity and Account within your organisation whatever the Entity type (individuals, companies, trusts, partnerships etc.). Its flexibility allows for the monitoring and reporting of all types of relationships, whether these are personal relationships, corporate groupings or a combination of the two.

Client static definition allows for the various images of documents that are produced by the customer to prove their identification and associate these images directly with their profile to be stored. This documentation can be aged and reviewed on a regular basis. All documents made available to kyc monitor are permanently held and aged, with specific review dates set by the user.

New documentation can be introduced at any time, and older documents can be replaced with more current versions. There is no limit to the number of documents that can be stored for each client. The system automatically raises "Issues" based upon missing documentation or documentation that has expired or passed its review date.

Typically, a bank or other financial institution will also require the customer to define their expected

usage profile during the initial CDD investigation. This may cover areas such as predicted average account balances, number of monthly transactions,

and types of business being transacted or geographic profiles of countries that the customer will be sending or receiving money from. It is essential to establish a legitimate business activity profile in order to check for suspicious activity. The system also stores and establishes recurring review dates for the customers, warning and enabling the user to conduct appropriate on-going reviews. kyc.monitor provides a
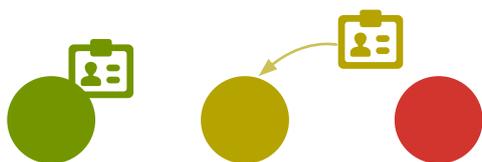
comprehensive solution to detect, analyse, and report suspicious activity that may be present within your daily transactions or transactions over user-defined periods.

Additional problems exist for the many institutions that originate from a country with a large overseas population when accepting cash for remittance back home. AML legislation requirements mean that this business type can often be risky and not worth taking

on.
kyc.monitor reduces this risk significantly by automating the associated workflow and compliance requirements. Details of the remitter, beneficiary and intermediary parties are maintained within the system along with all of their past transactions.

Risk profile

Under the recommended risk-based approach towards regulatory compliance, it becomes pertinent to initially assess and constantly monitor compliance risks that your customer base poses to your institution. This allows you to be proactive in mitigating risks that might be highly damaging to short-term profitability and long-term reputation of your organization.

Customer entities are categorised into risk-assessed groups called risk classes. Risk Classes are used to associate different rules and tolerances when evaluating transactions for suspicious activity. Risk classes can be developed to represent a simple high, medium or low rating or can match elaborate categorisations established by compliance policy. The user has two options when it comes to customer risk in our application. kyc.monitor can either import a risk calculated via the feeding system, or calculate its own risk value based upon user defined rules typically utilising risk based factors: Customer Type, Industry Type, Account Type/Activity Type, Country Rating (based upon FATF recommendations) and length of relationship Rating.

Profiles may be based on actual historical activity or upon the replies provided by the customer as part of the CDD process. kyc.monitor provides the compliance officer with the ability to monitor particular customers or accounts on a daily, weekly, monthly, or quarterly basis. A profile can be set to segregate and track cash transactions from non-cash transactions to meet regulatory mandates. Profiles may also be established for specific accounts and specific activity types to allow an organisation to choose the appropriate level of granularity on a customer-by-customer basis.

Trend monitoring

After establishing customer and account relationships and deriving appropriate profiles, transactional

activity must be captured to detect potential suspicious activity. kyc.monitor uses customer and account relationships and profiles together with daily activity received from your organisation's business systems to identify suspicious activity. Any activity that falls outside the norm and tolerance for a customer is "Red Flagged", highlighting the occurrence. Tolerances are user definable and based upon the risk profile of the customer.

Suspicious activity is raised as an "Issue", which is then passed to a review process. Compliance
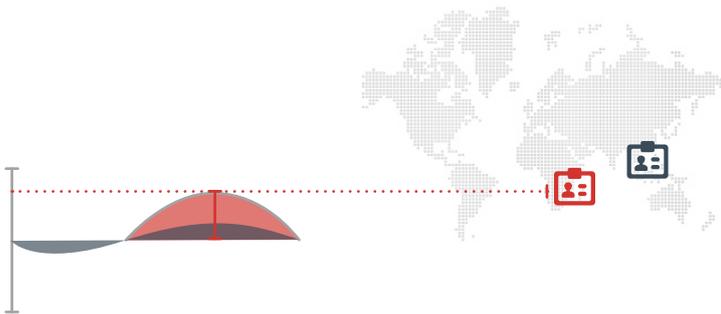
Officers and Account Officers can collaborate to reach a final determination regarding the validity of the reported suspicious activity. The various stages of the process are fully audited, thus demonstrating due diligence to the relevant authorities that your organisation is complying with the appropriate laws.

Ultimately, the reviewer will make a final determination with respect to the suspicious activity and update the case with that decision. In the event that transactions are deemed to be truly suspicious, the appropriate Suspicious Activity Reports (SAR) are produced. Cash Transaction Report (CTR) and Monetary Instrument Logs (MIL) can also be reported and produced for all cash transactions as required by the regulatory requirements. Other extensive reporting is available for managing the compliance process as well as for evaluating suspicious activity.

Legal investigations

In today's world climate, the search for those doing harmful and illegal acts has become increasingly more important. Financial institutions now play a vital role in the detection of such individuals and organisations by helping to identify their presence in transactions so that law enforcement officials can track them and/or cut off their sources of funds. Whether the request is a "314a" request from the

Financial Crimes Enforcement Network (FinCEN) or a subpoena/court order from another authority, it is the organisation's duty to fulfil the request for information to the best of their ability.

kyc.monitor provides functionality to address the major tasks in responding to requests for information:

- Importing information of requested parties

- Searching for the presence of customers and transactions that correspond to the request

- Examining the results of the search and determining which records are of interest

- Reporting/outputting of the desired search results.

Both transactional and Customer Static information may be searched to find appropriate items as required by the relevant legal framework. For example in the USA as part of a "314a" request, your organisation's Monetary Instrument Log (MIL) will be checked for appropriate activity over the previous 18 months. This may also include reporting on accounts opened and then subsequently closed within the period. Searches can be performed on several years of historical data, the limiting factor being the retention period of the data.
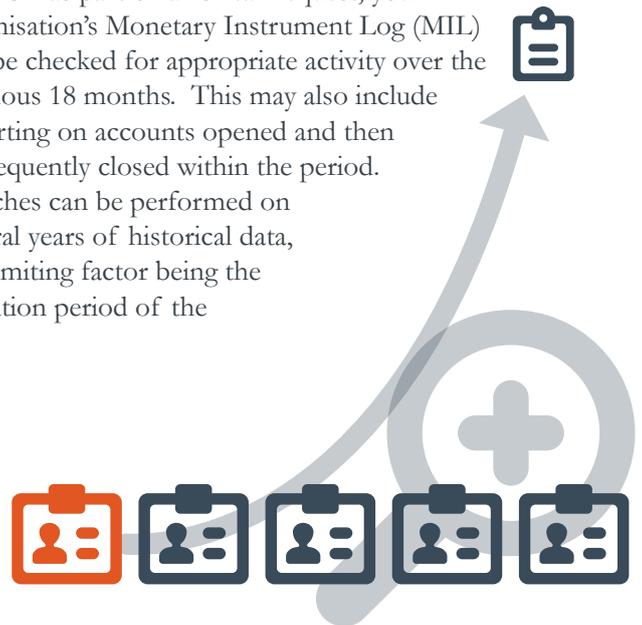
○ sanctions.

Find out more about why our customers are enjoying the benefits of corfinancial's sanctions solutions. How can we help?

call **0207 877 4045**
email **info@corfinancialgroup.com**
visit **corfinancialgroup.com**

solutions from

corfinancial.

london | boston | new york.

○ salerio.
Automates the flow of securities and treasury trades from matching through to settlement.

○ bitarisk.
Suite of applications addressing needs of private wealth managers, investment advisors, asset managers, quant teams.

○ paragon.
Fixed-income accounting hub delivers front-to-back office portfolio accounting and processing solutions.

○ sanctionsmonitor.
A sophisticated, easy-to-implement and easy-to-use sanctions monitoring, auditing and reporting tool.

○ abraxsys.
Comprehensive integrated banking platform delivering an industry-leading banking service.

○ costars.
Retail fund/transfer agency solution providing end-to-end administration for collective investments.

○ almeter.
Control financial and business risk by assessing the impact of varying interest rate scenarios and hedging activities.

○ kycmonitor.
Case managment solution to provide clear evidence to the relevant authorities that effective and sufficiently robust AML controls are in place.