ACAMS® TODAY
The Magazine for Career-Minded Professionals in the Anti-Money Laundering Field

Importance of data collection for a look-back

The term "look-back" in the regulatory world is usually meant for reviewing, analyzing and reporting the transactions of a financial institution for a specified duration of time due to internal control weaknesses. Typically, regulators require that a look-back be performed after an examination. Or the institution will be proactive and conduct its own look-back to scrutinize the transactions for various reasons. The financial institution (FI) discusses the parameters of the look-back with the regulatory authority based on the deficiencies found during the examination, and which often include:

- Length of the look-back period
- Type of transactions to be reviewed (e.g., only wire transactions)
- Type of transactions based on customer base (e.g., correspondent, bank-bank customers)
- Specific activity patterns around the type of transactions to be reviewed (e.g., cash-to-wire velocity, multiple originators wiring a common beneficiary)

A look-back project in general has the following stages

- Defining the requirements of the look-back
- Acquiring all related data for the specific duration
- Applying different rules based on risk rating mechanism to identify possible problematic transactions and creation of cases based on the results.
- Investigating the cases that are generated
- Filing suspicious activity reports (SARs) for the identified suspicious transactions after investigation.
- Report the findings of the look-back to the regulators and senior management

Hence, the FI should concentrate on the following

- Management and staffing the look-back project
- Collect transactional and related data for the look-back period
- Identify and acquire a suitable tool for performing the look-back that would be capable of
  - > Risk-scoring the customers
  - > Handling large data volume
  - > Analyzing the transaction for suspicious activity using methods like artificial intelligence, pattern matching and peering algorithms, and create relevant cases for investigation.
  - > Proper case management functionality to investigate transactions
- Define case investigation and workflow procedures
- Define SAR filing procedures
- Follow a well-defined quality assurance process
- Involve the regulators in the process and keep them abreast of the proceedings of the look-back

Since the process of a look-back is very expensive and could be drawn out, the importance of acquiring the transactional data for the specified duration should not be neglected. This paper emphasizes the importance of data acquisition on a Look-back project.

Data collection

Before the look-back project goes ahead full swing, the project manager and key members of the management team should spend sufficient time discussing the different data that would be required for the review.

The data collection process usually starts with identifying the data sources. The data for the look-back could be from multiple source systems. Once all of the sources are identified, then the data needs to be extracted using custom scripts or other utilities to format data so that they can be consumed by the look-back tool. Some look-back tools might come with pre-built utilities to extract data from certain standard core banking systems.

Data collection for the look-back

For a look-back project the following data is frequently required:

- Customer and account information including know your customer (KYC) information that existed during the specified duration and within the scope of the look-back
- Detailed historical transactional information for the specified period

The following are the potential challenges in acquiring this data:

- KYC information not available in electronic form: Some FIs may not have

Reprinted with permission from the June–August 2009 Vol. 8 No. 3 issue of *ACAMS Today* magazine, a publication of the Association of Certified Anti-Money Laundering Specialists

a good KYC system or have acquired a KYC system recently and hence the customer/account opening information might not be available in electronic format. In this case the FI would need to make available the paper copies of the KYC/account opening forms so that the investigation can be carried out effectively.

- KYC system does not have versioning capability: The KYC system installed at the FI may not have the capability to store all the historical information of a customer. This is important when performing a look-back as the investigators would like to see the information of the customer as of the time of the look-back period. If this is not available in the source system, then the FI should acquire the paper copies of the customer information and submit them to the look-back team to perform the investigation effectively.
- Stale data:
  - > KYC data may be out of date.
  - > KYC information may be incomplete for certain customers.
  - > Account opening forms are not readily accessible, particularly if the accounts have since been closed.
  - > Account relationships could have changed over the years.

These issues could be related to more generic problems within the FI and need to be resolved separately from the look-back project, possibly consuming a lot of time. For the purpose of the look-back, the FI needs to allocate resources to update the customers, accounts and the related data in order to effectively investigate the cases.

- Ensure data accuracy: Some of the data on the source systems might not be normalized or might not be consistently entered by all the users. Hence performing searches and look up on such data will not be efficient. Special care needs to be taken to identify these data elements during the extraction process and normalize the data where appropriate.
- New transactional system implemented over the years: When a new transactional system is implemented within the FI, the following cases may arise:
  - > The old system is archived and limited data is ported over to the new system. This data might fall directly under the purview of the look-back project.
  - > It is also possible that some of the data elements that are collected currently might not be available in the old system and vice-versa.
  - > When the data is ported over to the new system there might be some important information that does not have a place holder in the new system and hence is not ported.

In all the above scenarios, the FI needs to review the data elements, understand the importance of these for the purpose of the investigation and allocate resources to extract the information to the look-back tool.

- Database backups: Database backups are from an older version of the application and cannot be restored on the newer version for viewing the data. To resolve this, the FI may need to devise methods to extract the data directly from the backup database. The product vendors may be able to provide this service.
- Completeness of data: The FI may have multiple transactional systems and the core banking system is only programmed to receive the minimal information for booking the transactions. For example:
  - > Wire system may only pass the debit and credit entries to the core banking system, whereas all of the beneficiary, originator and country information are not passed.
  - > Some teller systems do not have the capability to provide details on mixed transactions information resulting in incorrect coding of transaction types, amounts and details.

To address this, the extract program should get all of the additional data from the source system (wire system, loan system, ACH system etc.) Care should be taken to avoid duplication of data, since the same transactions will be available from the core banking system.

- Multiple core banking systems: The FI might have multiple core banking systems due to geographic reasons, acquisitions etc. This could impact the data that needs to be collected for the look-back. The FI may then have to choose to extract information from multiple systems and just perform one look-back, or choose to perform separate individual look-backs. The FI needs to review all of the possibilities based on cost and ease of data extraction from the different core banking systems before proceeding with any approach.
- Ability to extract the data: Even if all of the information is available within the FI, the actual process of data extraction might become a challenge due to resource constraints, knowledge bank available, systems written in unsupported languages, timelines and many other factors. The FI should identify and enumerate all of these challenges and look at contacting vendors and third party contractors as an option to complete the look-back project successfully.

Data collection during the look-back

During the course of the look-back project it is important to collect the following data to keep track of the progress of the project and also to report back to the senior management and the regulators.

- Look-back summary
  - > Number of customers
  - > Number of accounts
  - > Number of transactions
- Case statistics
  - > Number of cases created
  - > Number of cases investigated
  - > Number of SARs filed
  - > Summary information of
- Number of customers, accounts and transactions for the review period
- Number of cases processed by investigator by period
- SAR statistics
  - > SAR
  - > Information on the SAR (i.e., category of suspicious activity reported, suspect information etc.)
  - > Number of SARs

The above data might be broken down by risk, customer types, location, department and period to provide more detailed drill down information.

Conclusion

Look-backs have become a part of the life within the AML world. The look-back will be more successful if you have good quality data. There will be challenges, but as long as they are identified and addressed, the FI will most likely end up with solid data. Applying the lessons learned from the look-back exercise will help improve the general AML governance of the FI.

Mahesh Viswanathan, CAMS, managing partner, Idola Infotech, LLC., Iselin, NJ, USA, mahesh@idolainfotech.com