The simplest request from an examiner can cause the heart of even the most seasoned Bank Secrecy Act (BSA) officer to race: “Let me see what that customer — or entity or account — has been doing over the past six months...” A look-back! Simple? Can be.

Whether you’ve been asked to conduct a look-back for a specific customer, a large entity or an account’s transaction history, it’s invaluable to be able to offer several approaches to satisfy the examiners’ curiosity and confirm unequivocally that the system you are using to monitor suspicious transactions is effective and comprehensive.

Flexible capabilities that allow you to respond to the examiner’s request with three types of look-backs will be critical to confirming that your monitoring is both accurate and comprehensive. These look-backs are:

1. A simple transaction history for a specific account that may include a single transaction type or all transactions over the period chosen, or
2. A defined money laundering (ML) routine (scenario), either existing or newly designed, run against the entire customer base or a select group, to identify and confirm that no suspicious transactions have been missed in the records under review, or
3. A transaction graph, which may include multiple entities with one or more transaction types, automatically displayed as a graph to facilitate interpretation of the data.

The ability to perform all three types of look-backs, for any period of time specified, quickly, easily and effectively may save your institution from the high costs and risks normally associated with institution-wide look-backs.

Difficulties during an exam that may indicate problems or inconsistencies in transaction monitoring may prompt the examiner to ask for a look-back on a specific account, a specific customer or a larger defined entity. The transaction(s) that the examiner may want to see could be specific (e.g., wire transfers to a customer over the last six months, or a combination of transactions that together may represent a suspicious activity, i.e., wire transfers to a customer in conjunction with ATM withdrawals). The inability to properly monitor this transaction combination, now popularly known as a classical terrorist financing pattern, would represent a serious deficiency in monitoring effectiveness and put the institution at risk of a full institution-wide look-back.

With many institutions, both banks and credit unions, conducting transaction monitoring by manual means, these simple look-back requests can turn into a time-consuming exercise fraught with risks. Long days become longer, costs escalate, other duties are ignored, and the risk to the institution grows by the day.
The inability to demonstrate that your transaction monitoring techniques are accurate and comprehensive may lead to more requests and risk, leading to a full look-back for many, if not all, customers and for many, if not all, transactions over a negotiated period of time. Expensive and risky for the institution.

Look-backs, narrow in scope, at the Bank Secrecy Act (BSA) officer level, may fall into the three categories previously described and conducted as follows:

**Simple transaction history**

A single entity or account that displays either a single transaction type or all transactions for a given account over a defined period. This is logically conducted through an inquiry function, wherein the BSA investigator, internal auditor or an examiner may ask to display the transaction history as defined. The following two diagrams illustrate the simple yet effective process in three simple steps:

1. Select the entity to be reviewed for the period in question
2. Enter entity criteria (e.g., account number)
3. Enter dates for look-back (e.g., six months) and select transaction history.

**Defined ML routine**

For more in-depth queries the examiners may ask that you conduct a look-back for a specific ML routine (scenario) run against a specific customer or a defined group over a specific period of time. This can be a daunting and time-consuming exercise for a manual system and for automated solutions that lack flexibility to readily and easily adjust parameters and customer “definition” as requested by the examiner.

Ideally, the BSA officer should be able to quickly select the criteria that defines the target customer, or entity, of interest and given the type of ML routine of interest the parameters must be easily defined. If necessary an entirely new ML routine designed in minutes may be most useful in demonstrating to examiners that your solution is effective and comprehensive. A flexible system should enable the following actions to be readily completed and once again demonstrate to the examiner that your transaction monitoring system is effective and comprehensive:

- Select customer criteria, broad or specific...
The inability to demonstrate that your transaction monitoring techniques are accurate and comprehensive may lead to more requests and risk, leading to a full look-back for many, if not all, customers and for many, if not all, transactions over a negotiated period of time. Expensive and risky for the institution.

Look-backs, narrow in scope, at the Bank Secrecy Act (BSA) officer level, may fall into the three categories previously described and conducted as follows:

- **Simple transaction history**
  - A single entity or account that displays either a single transaction type or all transactions for a given account over a defined period. This is logically conducted through an inquiry function, wherein the BSA investigator, internal auditor or an examiner may ask to display the transaction history as defined. The following two diagrams illustrate the simple yet effective process in three simple steps:
    1. Select the entity to be reviewed for the period in question
    2. Enter entity criteria (e.g., account number)
    3. Enter dates for look-back (e.g., six months) and select transaction history.

- **Defined ML routine**
  - For more in-depth queries the examiners may ask that you conduct a look-back for a specific ML routine (scenario) run against a specific customer or a defined group over a specific period of time. This can be a daunting and time-consuming exercise for a manual system and for automated solutions that lack flexibility to readily and easily adjust parameters and customer “definition” as requested by the examiner.

  Ideally, the BSA officer should be able to quickly select the criteria that defines the target customer, or entity, of interest. A flexible system should enable the following actions to be readily completed and once again demonstrate to the examiner that your transaction monitoring system is effective and comprehensive:
  - Select customer criteria, broad or specific
  - ML routine to define activity (e.g., wires in and ATM withdrawals)
  - Specify parameter values, minimum dollar amounts to monitor
  - Specify the time period for look-backs (e.g., previous six months)

  The results can be displayed as alerts with all transaction data available to graph as selected.

  An institution’s ability to quickly and easily comply with this type of Defined ML routine look-back request is a significant credibility builder for examiners, leading them to recognize that you have the transaction monitoring capability and flexibility to meet the high standards required for BSA/AML compliance.

- **Transaction graph**
  - A third approach to satisfying a look-back is useful by itself or as a supplement to those look-backs that generate a large amount of data. The effectiveness of the look-back results may depend on the ability to quickly interpret and analyze the results.

  This approach combines the ability to chart results from a look-back designed to monitor single or multiple entities or multiple transactions, and automatically graph results to facilitate interpretation in three easy steps as shown on the following diagrams:

    1. Select entity (e.g., account and enter account number)
    2. Enter dates of look-back (e.g., six months) and enter transaction codes of interest
    3. Select line chart or pie chart

  With these approaches to conducting look-backs during an exam or anytime the BSA officer or auditor wants to see historical transaction activities, institutions can readily demonstrate that they are indeed able to effectively monitor complex, multiple transactions by single or multiple entities. Such capabilities should establish the credibility of your BSA compliance program and avoid the time-consuming and expensive institution-wide look-backs prompted by doubts about your transaction monitoring capabilities.

Stephen O. Friend, CAMS, AMLP, vice president, sales, Focus Technology Group, West Peabody, MA, USA, Stephen.Friend@FocusTechnologyGroup.com