Paper SAS6800-2016

Alerts Don't Launder Money (or Finance Terrorism) – People Do!

Kathy Hart, Malcolm Alexander, SAS® Institute Inc.

ABSTRACT

For far too long, anti-money laundering and terrorist financing solutions have forced analysts to wade through oceans of transactions and alerted work items (alerts). Alert-centered analysis is both ineffective and costly. The goal of an anti-money laundering program is to reduce the risk for your financial institution, and to do this most effectively, you must start with analysis at the customer level, rather than simply troll through volumes of alerts and transactions. This paper discusses how a customer-centric approach leads to increased analyst efficiency and streamlined investigations. Rather than starting with alerts and transactions, starting with a customer-centric view allows your analysts to rapidly triage suspicious activities, prioritize work, and quickly move to investigating the highest risk customer activities.

INTRODUCTION

Money laundering is the process of making illegally gained proceeds appear legal. To protect the financial system from "the abuses of financial crime, including terrorist financing, money laundering and other illicit activity", the United States established the Bank Secrecy Act (BSA) in1970. The European Union established directives on anti-money laundering in 1991. These statutes and the follow-on legislation require banks and other financial institutions to report suspicious activity to the appropriate authorities.

These legislations require financial institutions to implement an Anti-Money Laundering Compliance Program to monitor for suspicious activity and then file Suspicious Activity Reports (SAR) in the U.S. Other countries have their own set of reports that they must file. Financial institutions use software to automate monitoring and to generate alerts when suspicious activity occurs. Analysts investigate the alerts and decide whether to close the alert or to create a case for an investigator to review and disposition. The investigator gathers additional information before deciding whether to close the case or file a SAR.

SAS® released its first anti-money laundering solution, SAS Anti-Money Laundering, more than 10 years ago. SAS Anti-Money Laundering uses scenarios to generate alerts that are then reviewed by the analysts.

The solution has evolved with the ever-changing landscape of the global market. Originally, Anti-Money Laundering Compliance programs focused on dispositioning alerts, which represent granular behaviors, such as out-of-footprint ATM activity. Overtime, money-laundering techniques have become more complex and the regulatory landscape has changed. Creating more scenarios for a broader monitoring program are now the norm. These changes result in an all-time high for alert generation.

As a result of these changes, a more holistic approach to investigating money laundering is required. This paper presents some major changes and improvements to SAS Anti-Money Laundering that make detection more meaningful, triage and investigation more efficient, and greatly simplify the day-to-day management of Anti-Money Laundering Compliance programs in financial institutions.

TRADITIONAL ALERT TRIAGE AND CASE INVESTIGATION

STANDARD TRIAGE AND INVESTIGATION PROCESS

The goal of this effort is to come to a decision as to whether to report a customer or external party that does business with the bank (both referred to as an entity), as suspicious.

Figure 1 shows the general process:

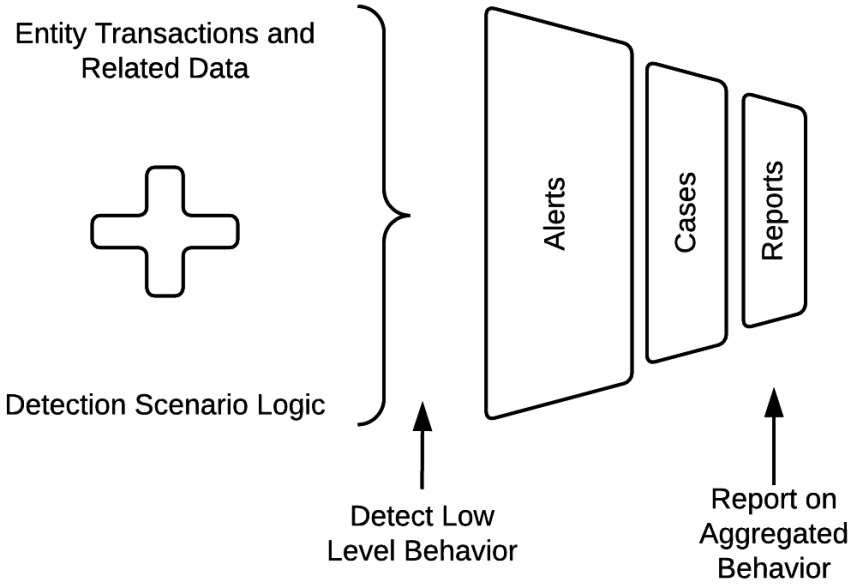

Figure 1. Typical Transaction Monitoring Process

In a typical process, the software uses entity and scenario information to generate alerts that represent suspicious behavior at a granular level. Table 1 contains examples of granular alerts generated by Anti-Money Laundering scenarios.

Table 1: Example Alerts

Alert Level	Alert Category	Alert Type	Alert Description
Account	Cash	Structured Withdrawals	An account has multiple large withdrawals over a short period.
Customer	Watch list	Politically Exposed Person	A customer is designated as a politically exposed person (PEP) on a watch list
Household	Cash	Large Cash Deposits	Customers in a household have a daily total amount of cash deposits that exceed a threshold
Associates	Other	Balance Inquiry	An associate performs a large amount of balance inquiries
External	Wires	Multiple Internal Beneficiaries	A single external remitter wires money to multiple internal beneficiaries.

Analysts then use an application to review, or triage these low-level alerts, working to determine whether the detected transactional behavior is worthy of a deeper investigation. The alerts generated are associated with customers, accounts, households, associates, or external parties. If it is determined that the alert requires additional review, the analyst creates a case.

Cases bridge the divide between low-level behavior detected by automated systems, and the regulatory report that is filed on an individual or organization. Investigators trained in the research and analysis required to detect suspicious behavior perform the more complicated work required for cases. Where

analysts traditionally look at an alert and its associated transactions in relative isolation, investigators pull together the whole picture of individual or group activity related to money laundering or terror financing.

Herein lies the major challenge. Given the growing sophistication of criminals, we detect granular behavior, but ultimately report on the aggregated behavior of people, groups of people, or organizations.

CHALLENGES WITH THE TRADITIONAL WAY

The mismatch between the ways that we detect and how we report has important consequences. On the business side, a financial institution risks under-reporting because at the beginning of the process, triage, analysts miss broader patterns of behavior that span alert types. Even with additional training and best practices, analysts must actively search out other alerts related to the entity under review. This is a manual process and thus prone to errors. Overly conservative analysts create extra work for investigators, pushing alerts on legitimate transactions (also known as false positives) to cases. In this process, investigators are the first to take a holistic look at the entities, which increases their workload.

Since dispositioning each alert individually is time consuming, tuning the scenarios to reduce the number of false positive alerts is very important. However, tuning scenarios to reduce false positive alerts can actually suppress the generation of alerts on truly suspicious activities.

Financial institutions deal with the workload issues in a variety of ways – none of them optimal. Some organizations organize by alert “type”, for example, routing all wire alerts to a special sub-team. This, and various other ways of organizing around alerts has the side effect of causing workload balancing headaches – and is still subject to the risk of missing aggregate behavior. Others create “super-alerts” in an effort to bend an alert-oriented system to the need for broader investigation. This causes some loss of visibility of the important lower-level behavior, and its efficacy is subject to the degree to which you can automatically roll up behavior to a meaningful super-alert.

On the technical side, systems built end-to-end around granular behavior tend to be cumbersome and difficult to use when trying to synthesize information for the purposes of investigation. Built around the alert, facilities for quickly navigating to other entities, switching back-and-forth to gain a broader understanding of behavior, or viewing both detailed and broader behavior can be unwieldy. Visualizations of alert-level information are not as useful as they might initially appear.

In summary, the implications of working with alerts, but reporting on entities, are far-reaching and touch many areas of a BSA program. The remainder of this paper draws on these organizational and technical lessons to propose a new approach, which is being implemented for SAS Anti-Money Laundering 7.1.

A BETTER APPROACH

A change in philosophy to make people the focus, from the beginning, resolves many of the challenges. Figure 2 shows the new philosophy.

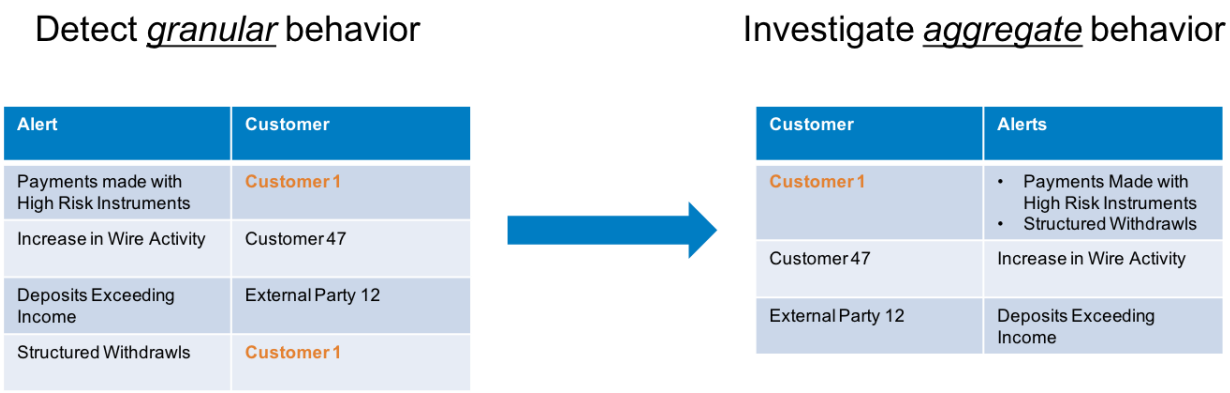

Figure 2: Entity Triage

The goal here is to retain the benefits of detecting low-level behaviors, but gain the ability to look holistically at an entity and quickly come to a decision as to whether their overall behavior is suspicious. Beyond just new reports and aggregations, moving to this philosophy has implications for the processes that generate alerts, and opens up new opportunities to provide much more streamlined and efficient user interfaces. This makes analysts and investigators more productive.

ALERT GENERATION

SAS Anti-Money Laundering is known for its white-box approach to transaction monitoring; financial institutions globally use customizable out-of-the-box scenarios, or develop their own scenarios to detect granular behavior. The engine of this detection process is the Alert Generation Process, or AGP.

The AGP examines entity transactions and related data, running scenarios to generate alerts. Transitioning to an entity-centric view affects numerous parts of the AGP.

Aggregation

After the alert generation is complete, the alerts are aggregated to a customer, associate, bank, or external party for further investigation and disposition. Aggregation rolls up account alerts to the primary owner of the account and household alerts to the head of household. After aggregation, triage of all alerts is possible by reviewing people or organizations. Table 2 shows the rules for aggregating alerts to entities.

Table 2: Alert to Entity Mapping

Alert Type	Entity to which alerts Aggregated
Account	Customer
Customer	--
Household	Head of Household Customer
External Party Account	External Party
Bank	Bank
Associate	Associate

Replication of Data

Investigating an alert includes investigating transactions associated with the alert. This includes not only the transactions that cause the alert but also other related transactions. Replication is the process of gathering the related transactions for investigating and archiving. Changing investigations from alerts to people means investigating transactions related to the suspicious people. For account alerts, replication gathers all transactions associated with the primary account owner and not just transactions associated with the account. For household alerts, replication associates transactions from all accounts in the household to the customer defined as the head of the household.

Alert Routing

Since investigators no longer receive individual alerts, routing of alerts to investigators based on alert type rules is no longer necessary. Instead of matching alerts with specialists, automatic routing is available for workload balancing. A round robin assignment method determines the assignment of customers and other entities with alerts to investigators. The assignment maintains ownership of existing entities in triage and assigns new entities to investigators in alphabetical order.

Routing of aggregated information allows more well-rounded analysts versed in a variety of suspicious behavior to produce effective and productive cases.

AGP Summary

Aggregation, replication, and routing are challenging for customers or consultants to bolt-on; the system has to be built with this in mind, which is the major effort related to the AGP in SAS Anti-Money Laundering 7.1.

USER INTERFACE

SAS Anti-Money Laundering 7.1 extends the entity triage component of SAS Anti-Money Laundering 6.3m1 to provide a completely new interface to take advantage of the aggregations provided by the AGP. A few key principles drive the design of the new user interface:

- Leverage the aggregated information to display holistic views of entities.
- Display the most critical information prominently, focusing on those items key to making decisions.
- Simplify and flatten navigation, allowing a variety of entities and other objects to be viewed at the same time

Holistic Views

Rather than reviewing individual alerts, the Triage component for example, provides aggregated views. Figure 3 shows the entity triage list.

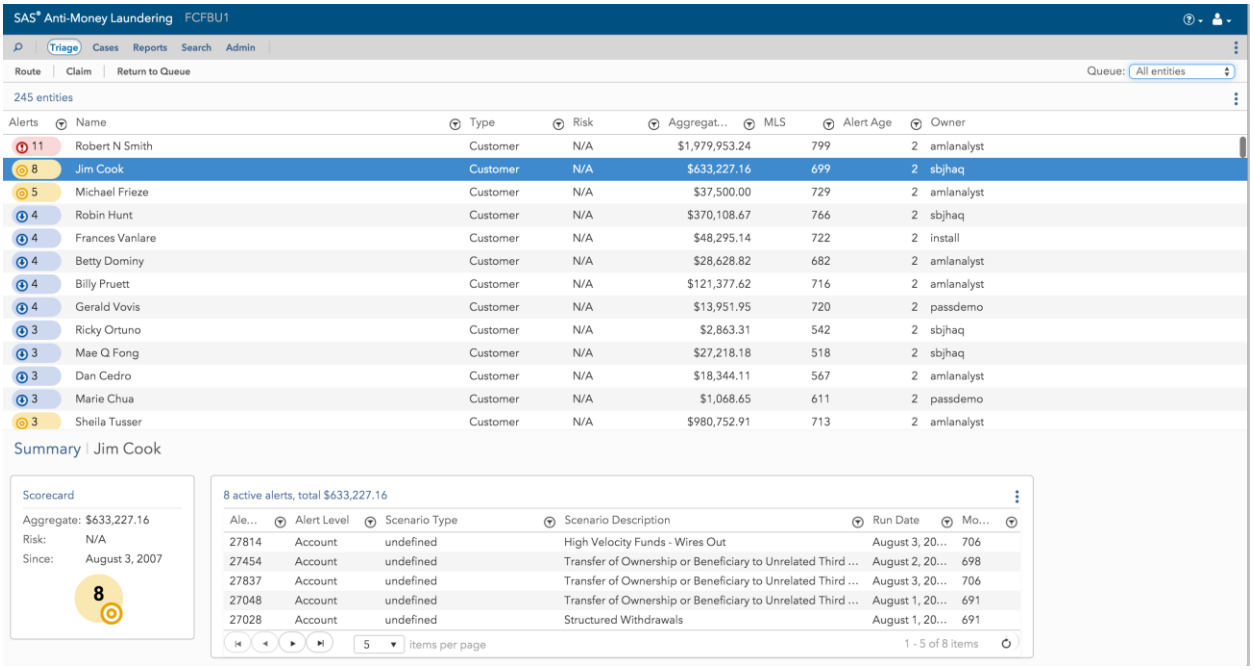

Figure 3: Entity Triage

Rather than prioritizing by alert type, new metrics are available to better quantify risk to your institution across all entities, whether they are internal customers, external parties, or any of the other types noted in Table 2. The user can customize the prioritization through filtering and sorting of the metrics. The application retains these settings across user log-ins, and provides an option to reset to the defaults. Selecting a row in the detail screen shows a summary, at the bottom of the screen, of the underlying alerts. Double-clicking on a row displays the detail page

Focus on Decision Making

Each page in the application presents the most useful information for making a decision at a particular time. The customer detail screen shown in Figure 4, for example, displays all the open customer alerts, linked to the transactions table at the top.

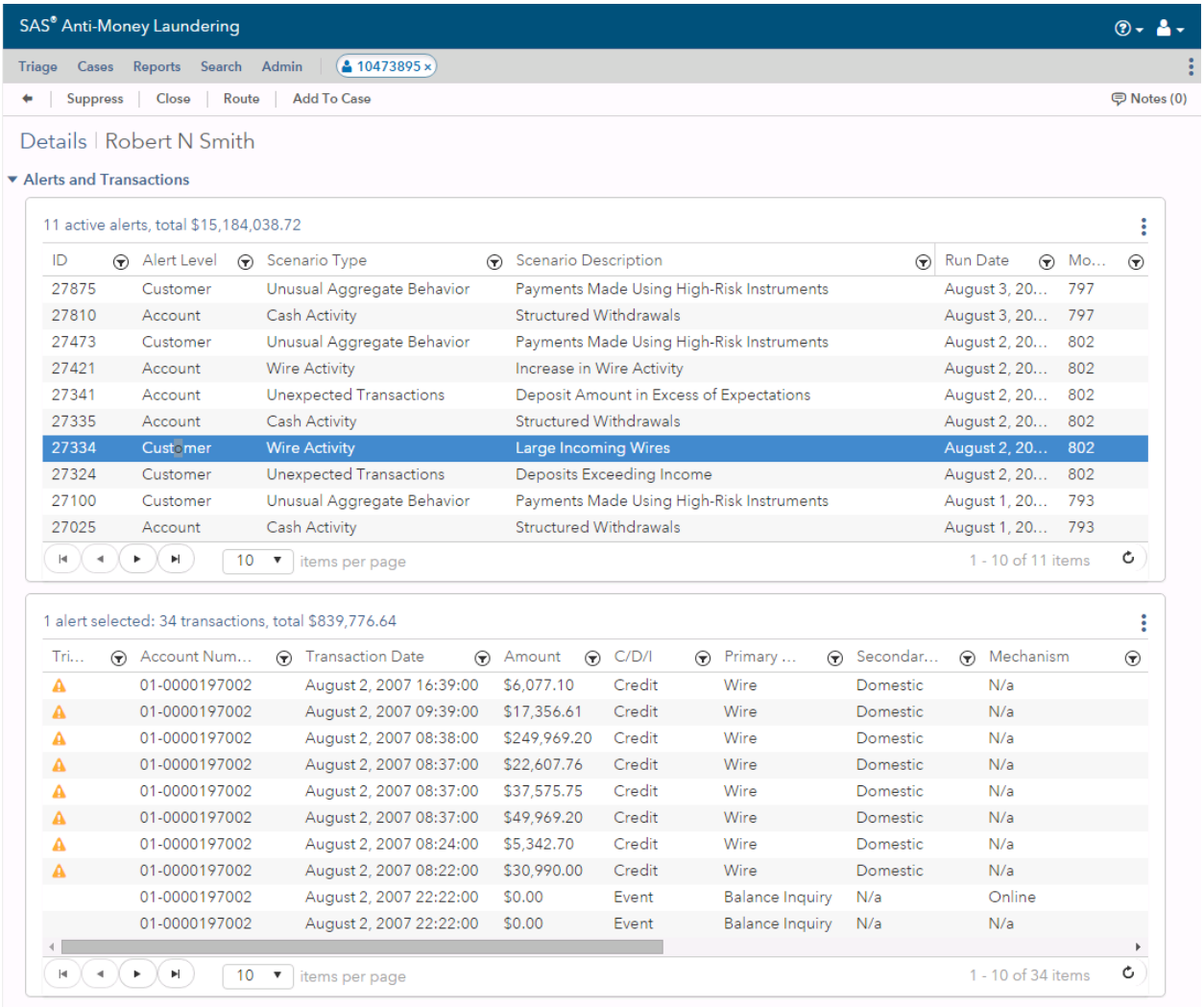

Figure 4: Customer Alerts and Transactions

Selecting an alert dynamically changes the transaction view to filter to the triggering and related transactions for that alert. De-selecting an alert brings back the view of all the transactions available. With these linked tables, users can quickly find transactions of interest. Demographic information, typically found at the top of the page in most applications, is less important to the actual decision and thus placed farther down the page.

Navigation

Systems designed around alerts tend to use a strict page hierarchy that encourages drill-down, and are not optimized for reviewing a variety of different entities at once. SAS Anti-Money Laundering 7.1 flattens the navigation to allow users to see and access a variety of information very quickly. The screenshot in Figure 5 highlights some of these features:

- Main areas of the application are always available with one click (Triage, Case, Report, and so on.)
- A variety of items can be open at the same time, and are cached to avoid repeated database calls and performance challenges. For example, a Customer, a Transaction, an External Party, and an Account detail page can all be open and users can switch back-and-forth easily – without having to leave the case or triage item that they are working on.
- Any actions that the user can take are always available, regardless of where you are on the page. Pages scroll vertically to provide quick access to lots of information. The menu bar with buttons like “Suppress” and “Add to Case” are “sticky” – that is, they are always available at the top of the screen.

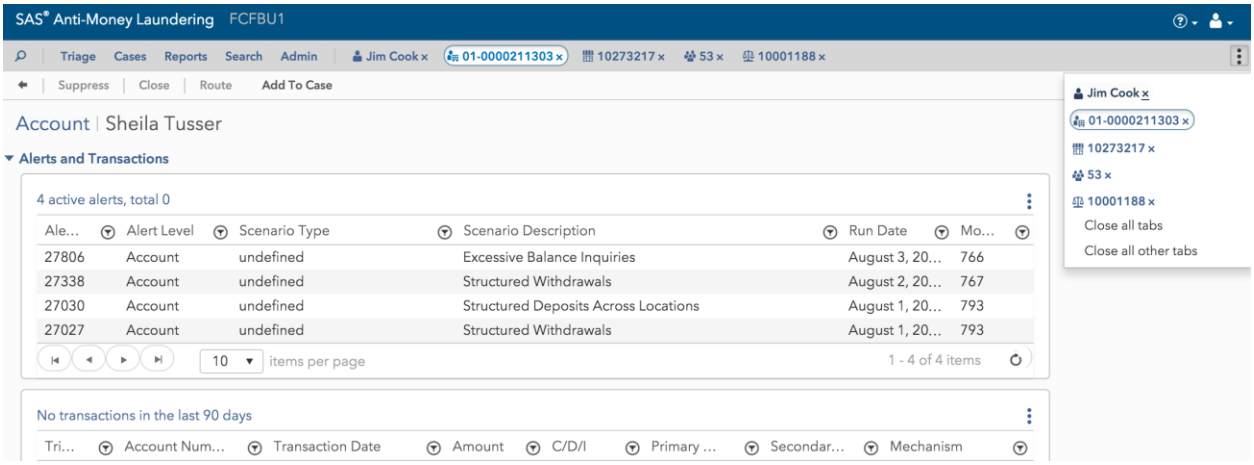

Figure 5: Navigation Methods

CONCLUSION

The compliance space has transitioned from an era of process adherence to an era that places great demands on the ability of organizations to identify complex activities by possible multiple actors. Working at the level of the individual alert is no longer viable, and SAS Anti-Money Laundering 7.1 makes BSA organizations more effective.

ACKNOWLEDGMENTS

Thanks to Brian Ferro and Dan Tamburro.

CONTACT INFORMATION

Your comments and questions are valued and encouraged. Contact the author at:

Kathy Hart
Kathy.Hart@sas.com

Malcolm Alexander
Malcolm.Alexander@sas.com