Utilizing the Suspicious Activity Report Audit as a Diagnostic for a Financial Institution’s AML Program

Author: Michael S. Schidlow, Esq., CAMS-Audit, CFE

Disclaimer: The views and opinions expressed in this paper are those of the author’s and do not reflect the official policy or position of any financial institution.
I. Introduction and Background

The underlying purpose of a suspicious activity report (SAR) is for a financial institution or other obligated entity to report suspicious activity that may be reflective of a predicate crime. Banks are required to report suspicious activity that may involve money laundering, Bank Secrecy Act (BSA) violations, terrorist financing and certain other crimes above prescribed dollar thresholds.¹ U.S. guidance states that “banks are not obligated to investigate or confirm the underlying crime (e.g., terrorist financing, money laundering, tax evasion, identity theft and various types of fraud). Investigation is the responsibility of law enforcement. When evaluating suspicious activity and completing the SAR, banks should, to the best of their ability, identify the characteristics of the suspicious activity.”² To the more seasoned anti-money laundering (AML) practitioner, this statement feels at odds with the direction that many recent enforcement actions have taken. The challenge being that “[o]ne purpose of filing SARs is to identify violations or potential violations of law to the appropriate law enforcement authorities for criminal investigation. This objective is accomplished by the filing of a SAR that identifies the activity of concern.”³ And yet, financial institutions do not always have the operational foresight to match an enforcement action’s hindsight.

Looking at the action taken against JPMorgan Chase (JPM) in 2014 as an example, the then-largest ever financial crime compliance (FCC) related penalty was assessed based on the bank’s inability to piece together a larger picture about one client’s crime in specific. In January 2014, the Southern District of New York announced the imposition of a joint enforcement action between their offices and other bank regulators against JPM. This deferred prosecution agreement and consent order was the direct result of the bank’s felony violations of the Bank Secrecy Act (BSA) relative to one account holder—Bernie Madoff’s business.⁴ Prosecutors argued that “the Madoff Ponzi scheme was conducted almost exclusively” through various accounts held at JPM and drew a direct line between Madoff’s fraud and the bank’s oversights, citing the bank for “repeatedly” ignoring warning signs.⁵ “The bank connected the dots when it mattered to its own profit, but was not so diligent otherwise when it came to its legal obligations,” said Preet Bharara, the U.S. Attorney for the Southern District of New York.⁶

¹ Federal Financial Institutions Examination Council (“FFIEC”) BSA/AML Examination Manual Examination Procedures, Suspicious Activity Reporting – Overview, Page 60
² FFIEC BSA/AML Examination Manual Examination Procedures, Pages 67-68, Identifying Underlying Crime
³ FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, Page 68, SAR Filing on Continuing Activity
⁴ “JPMorgan is Penalized $2 Billion Over Madoff”, Ben Protess and Jessica Silver-Greenberg, New York Times, January 7, 2014
⁵ Id.
⁶ Id.
Among other facts that came out as a result of the enforcement action was that Madoff Securities’ know your customer (KYC) profile was incomplete and/or incorrectly completed, there were a reported two transaction monitoring alerts in the lifespan of the Madoff Securities customer relationship, and the only SAR that was ever filed in the U.S. was done only after the Madoff’s arrest.\(^7\)

Frequently, when those in the audit function reflect on the gravity of a SAR, the primary consideration is centered on mitigating regulatory risk exposure. The focus for most SAR audits will deal with how transaction monitoring leads into alert processing, where alert processing leads to investigation, some quality control-centric reviews of filing categories, and end-to-end workflow. Auditors are quite correct to be concerned with these factors.

In addition, a well-executed SAR is very much the health indicator of how well an institution’s four pillars\(^8\) approach is working. Alert processing speaks to transaction monitoring, and the SAR form will reflect a strong (or weak) KYC file. The SAR reporting categories and narrative will correlate to appropriate AML staffing levels, qualifications and training to the red flags. Consistency in the quality of a SAR could speak to the strength of the internal audit function.

As independent as audit can be is as broad as risk exposure gap exists when it comes to understanding the fundamental nature of SAR filing. Many AML auditors can readily recite the framework and guidelines for filing requirements. However, absent hands-on experience in alert management through case dispensation, the challenges, frustration and rewards of a thorough investigation can get lost in the regulatory mire. While many auditors do review AML sensitive matters, in a manner of speaking, the focus tends to be on the procedural “hows” of SAR filing.

SAR reports contribute critical information that is routinely analyzed, resulting in the identification of suspected criminal activity and the initiation of investigations, as well as the identification of significant relationships, trends and patterns. The reporting also expands the scope of ongoing investigations by “pointing to the identities of previously unknown subjects, exposing accounts and hidden financial relationships, or revealing other.”\(^9\) Most

\(^7\) JP Morgan Chase Bank, N.A. Deferred Prosecution Agreement, Exhibit C, Statement of Facts, Page 5, Section 21; Page 19, Section 85

\(^8\) “Four Pillars” is meant to colloquially reference the compliance with the four key requirements of Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) Act of 2001, Pub. L. No. 107-56, 115 Stat.272 (2001) [hereinafter USA PATRIOT Act] (codified in scattered titles of U.S.C.), Title III, Section 352, generally being a system of internal controls, policies and procedures, a designated Bank Secrecy Act/AML compliance officer, ongoing training, and independent testing of the AML program.

\(^9\) FinCEN Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance, FIN-2014-A007, August 11, 2014
importantly, these reports identify the previously hidden currents by which illicit actors finance their unlawful activity.\textsuperscript{10}

Auditing SARs as not only a regulatory benchmark, but based on their potential level of utility to law enforcement is a rational basis for auditing SARs. That mindset is, in part, now part of a formalized advisory issued by the U.S. Financial Crimes Enforcement Network (FinCEN). Thus, examining SARs through this lens will then lend a view to whether or not all of the SAR’s composite pieces that are drawn from the institution’s AML program (transaction monitoring, KYC, investigative, documentation, form, narrative, quality assessment) have that same level of functionality.

Modern, adaptable and successful SAR audits need to consider not only regulatory efficacy but also the weight of the institution’s filing regime in terms of detecting and deterring the actual predicate offenses. This paper will serve to explore the correlation between a strong SAR audit process and the appropriate detection and reporting of a client’s suspicious activities.

\textbf{II. The SAR Form}

There are two principle considerations in auditing the SAR form. The first is data flow integrity, which is meant to describe how data from the institution’s system of record auto populates in the SAR form. The second is manual data input. Both considerations are crucial, as the form is a symbiotic representation of both types of data. From an auditor’s perspective, however, they must be diagnosed separately.

\textit{Data Flow Integrity}

FinCEN has reported that almost 11,000 users in both the regulatory and law enforcement conduct roughly 30,000 searches per day for making queries about known subjects. Law enforcement in specific is utilizing that database in order to either commence or enhance an ongoing investigation of a suspect.\textsuperscript{11} A preponderance of those queries are carried out by “form search,” where law enforcement will search SAR form data for specific information such as a tax identification number, Internet protocol address, or reporting category. This is done because it “would be difficult, time-consuming and costly, for law enforcement doing widespread searches of the database for particular field data, to hunt for these data in narratives, on the chance that filers placed important information in the narratives rather than in the correct

\textsuperscript{10} Id.

\textsuperscript{11} Id.
Accordingly, the integrity of the data in the forms is absolutely crucial to law enforcement, and is equally as significant in determining the SAR filing process’s success. Yet, SAR form data is quite frequently the largest proportionate source of errors. An excerpt from a 2010 Treasury Inspector General’s Audit report reflects the following:

“We found that 59 percent of the SARs filed in fiscal year 2006 had data quality problems (missing, incomplete, inconsistent, or inappropriate information) in one or more fields critical to law enforcement. The preponderance of problem SARs were filed by MSBs (approximately 428,000) and depository institutions (192,000). The critical fields most often containing missing or erroneous data related to the subject, including name, address, or identifying information. We believe these SAR data quality problems diminish the usefulness of the data for FinCEN, law enforcement, and other users....We also observed certain blank SAR fields for information that the filing institution should clearly have had available, such as the type of suspicious activity observed, the institution’s address, or the address of the suspicious transaction. Furthermore, we observed significant variation in the percentage of SARs with missing data among similar depository institutions, which raises questions about the diligence of certain depository institutions when filing.”

From the auditor’s seat, these types of discrepancies could speak to one of two root causes: automatic data feed or manual input errors. Automatic data feed and integrity flow errors, meaning data that auto-populates from the system of record into the SAR form field) are more readily detectable. These types of errors will be consistent and present to an auditor as an issue common to all of the SARs sampled. One example of a data flow integrity could be where the data is stored in the system of record as text format, but the form/SAR platform will “read” that data to have a numeric value, similarly as a misclassified field would in Microsoft Excel. For example, if a nine-digit tax identification number starts with zero, the data feed mechanisms may erroneously read that as a zero-value integer numerical and eliminate it from the form field. Again, an error of this nature would present consistently across all of the SAR forms which are sampled. A similarly, though less commonly occurring issue which speaks to the integrity of the SAR form is data shift, where when all or portions of an entry for a data field included in data files

---

12 SAR Data Quality Requires FinCEN’s Continued Attention, Pages 12-13, Office of the Inspector General, Department of the Treasury, January 19,2010, OIG-10-030
used to upload SARs appear in the positions reserved for other data fields. These typologies of error likely have a root cause in a SAR reporting platform, which was purchased off the shelf and not tailored closely enough to the financial institution’s systems.

**Manual Data Input and Selection Errors**

For a SAR auditor, the far more telling and significantly more egregious type of errors are manual input and reporting category selection. Manual data input errors can include typographical errors, transposition errors, or other incorrect data being included in the form. From a sampling of SARs, it may be useful to see if all of the manual input errors are coming from one or two SAR filers under review, as this may indicate that they are not equipped with the right training or resources to complete their role. However, at a broader level, if an auditor is reviewing the work of all of the FIU/SAR writers’ team and sees continual manual data input errors then there is generally one root cause: the SAR team is understaffed in comparison to the number of alerts that are being generated and they are being rushed into dispositioning those alerts. It is impossible to universally qualify how many alerts every business at every financial institution should generate, but reviewing a case study helps frame the audit consideration.

When FinCEN issued a Civil Monetary Penalty against Wachovia Bank in 2010, one of the key findings centered on alert generation to SAR filing ratio. The enforcement action noted “[t]he Bank placed greater emphasis on clearing alerts and eliminating backlogs than reviewing and reporting possible suspicious activity,” which was based on a reportedly overwhelming number of alerts being generated by a poorly calibrated system. One potential indicator for Wachovia would have been to examine the quality of the SARs that it was issuing, as they would have likely reflected a number of manual data input errors indicative of the understaffed SAR filing team at the time, who are trying to clear as many alerts as possible.

**Category Selection**

One commonly cited issue is that the category of reported suspicious activity (check fraud, identity theft, money laundering, etc.) does not correlate to the activity described in the narrative. The selection of reported activity should be consistent between teams of SAR filers, if not uniform throughout the

---

13 Id. at Page 25
14 “Each alert or event on an international correspondent bank generated by the Bank’s automated transaction monitoring system was comprised of as many as 30,000 individual transactions (with an average of 1,400 transactions per alert), which rendered the monitoring system practically unmanageable. The monitoring system was routinely tuned so that the number of alerts generated by the system with respect to international correspondent banks remained constant at around 300 each month.” - Assessment of Civil Monetary Penalty, Wachovia Bank, NA (2010), FinCEN Number 2010, Pages 4-5
institution’s SAR filing arms. The confusion of categories (e.g., identity theft versus account takeover) should indicate to an auditor that either the FIM does not contain those definitions for reference, or that there is a lack of training around the use of reporting categories. As training is a key control, this type of an audit finding is reflective of a “pillar” failure (meaning inconsistent or insufficient training) and thus a very high-risk finding.\textsuperscript{15} This issue comes to light most prevalently where the SAR filer is uncertain of which reportable category they should be selecting and opt for the “other” field on the SAR form. They should optimally input what they believe to be the appropriate category of offense. There are very few better benchmarks for an auditor to determine the efficiency of an institution’s FIM and training (both key controls) than the “other” field. Reviewing data from the same previously referenced Inspector General’s Audit Report found that “the suspicious activity was often characterized incorrectly or not at all. For example, we identified approximately 65,000 SARs (approximately 64,000 MSB SARs and 1,000 depository institution SARs) with “other” selected but either no description or an invalid description of the activity...we noted suspicious activity described as a string of numbers, the words “not sure,” “who knows,” “nothing suspicious,” or other similar and meaningless information.”\textsuperscript{16} Incongruities in the “other” field can readily disclose to the auditor that the SAR writer is describing an existing reportable offense but does not have the resources to rely on for that definition.

Again, at the most fundamental level SARs are used by law enforcement on current or emerging cases, and the erroneously reported information can greatly diminish the value of SARs to law enforcement. Moreover, these investigators have a clear line of communication to bank regulators. As such, law enforcement are often the first set of external reviewers who can determine and in some cases report these inconsistencies (and their frustrations with them) directly to a regulator. This is why it is crucial to audit the various reporting categories for consistency as a hallmark of AML understanding throughout the institution.

III. The SAR Narrative

While U.S. guidance provides that the SAR narrative “provides a sufficient description of the activity reported as well as the basis for filing,” functionally the narrative can be highly critical for law enforcement.\textsuperscript{17} Far too frequently, auditors can become too focused on the narrative’s quality against their institution’s benchmarking process while not stepping back to appreciate the

\textsuperscript{15} USA PATRIOT Act, Title III, Section 352
\textsuperscript{16} SAR Data Quality Requires FinCEN’s Continued Attention, Pages 17, Office of the Inspector General, Department of the Treasury, January 19, 2010, OIG-10-030
\textsuperscript{17} FFIEC BSA/AML Examination Manual Examination Procedures, Page 69, SAR Completion and Filing
gravity of a well (or poorly) written narrative. A narrative can drive a prosecutor’s ability to glean chargeable offenses by outlining to a degree the underlying elements of a crime, jurisdiction, statute of limitations, and even the availability of supporting forensic evidence. Understanding this principle and then auditing, where possible, to the same will help ensure SAR consistency as well as SAR utility.

One key way to potentially drive consistency and efficacy in the SAR filing process is to both train to, as well as audit to, the elements of the predicate offenses being reported as they relate to the red flags of the reported unusual activity. Common transaction monitoring scenarios include terms akin to “sequentially numbered items” or “activity not commensurate with the customer’s anticipated activity;” those scenarios are symptomatic of crimes but not underlying elements. Very frequently, SARs will then be filed utilizing generalizations of the activity which does not include the specific details of a) the type of the activity and b) a reflection of the true legal elements of a crime.\(^{18}\)

Take, for example, the crime of check fraud. Paraphrasing the essential elements of this offense, an actor issues a check which they know or have reason to know does not have sufficient funds to cover the amount. The check must be presented to another party for cashing or deposit.\(^{19}\) Transaction monitoring for this type of offense might reflect a groomed/dormant account with nominal transactions, followed by a massive influx of check deposits, culminating in large and under the reporting threshold cash withdrawals/point of sales purchases. In a hypothetical case scenario, if the narrative simply presents generic facts that “a check returned (i.e., bounced)” on the subject’s and that this is unusual for that client’s anticipates use little value is delivered. Conversely, where the investigator/analyst can identify the nature of the check fraud with specificity (e.g., forged endorsement, altered payee, forged maker, etc.), by framing the narrative to those specifics, would greatly aide law enforcement in establishing the essential elements during their investigation.

Auditing a sample of SAR narratives against the essential elements or functional elements of a crime would allow the auditor to identify consistencies. Building from the example of check fraud, an auditor reviewing the reported activity to the elements of an underlying offense would allow them to verify whether a single report’s narrative adequately supports the investigator’s conclusions about that offense, and consequently would allow

\(^{18}\) The elements could be utilized as a reference, but there is no regulatory obligation to report/narrate to the elements of the crime. Please refer to appropriate guidance for SAR filing parameters.

\(^{19}\) New York State Law, Penal Law, Part 3, Title K, Article 190.00-190.15
the auditor to see if SAR writers are all reporting the unusual activity as the same reportable predicate crimes.

The narrative must further reflect consistency in the filing process. The narrative’s language should adroitly articulate the red flags with the understanding that they can be relied on by law enforcement to establish the essential elements. Inversely, the predicate activity described in the narrative should mirror the selected boxes indicated in the SAR form. Anecdotally, auditors may encounter a SAR form indicating that a client was the victim of “unauthorized electronic intrusion.” However, the narrative reports, in exquisite detail, that the client is in reality the victim of a wealth management account takeover by listing the jurisdictional elements of wire fraud, identity theft, and account takeover. By comparing the selected reporting activity to that narrative, it may appear, at a superficial level, to be a match. However, at the regulatory and even prosecutorial level they are entirely distinct offenses. Consistent narrative-centric failures can and have been the source of previous regulatory findings (e.g., In the Matter of American Express Bank International).

While this approach could be more definitive for fraud-related SARs, it is less so for money laundering related activity. For most institutions the money laundering specific SAR is issued because the activity is unusual and, in sum, has no other likely explanation but to be illicit activity. In an instance where there is no other reported activity besides money laundering, the auditor’s objective should be to ensure that the activity is concisely explained. A narrative that, as best as possible, described the “boots on the ground” activity of the SAR’s subject greatly aides law enforcement in knowing whom to pursue, which agency could pursue that person and what other resources they may need in their investigation. Moreover, as the likelihood of an account being utilized for all three stages of the money laundering cycle is nearly impossible, the narrative should deliver the end-to-end disposition of those funds within the account. If, for example, the activity involves deposits in numerous geographies that may indicate to law enforcement that it is drug trafficking proceeds as compared to trade manipulation. To that end an auditor reviewing a SAR narrative should be able to, simply by reading the narrative, watch the money trail and determine that the institution followed the flow of the potentially illicit funds. Validating this storybook review of a narrative will add tremendous value to law enforcement officials who wish to trace the illicit

---

20 An activity where, for example, a client’s personal email account is compromised, then a wire transfer request is issued by the fraudsters who compromised that account to the client’s wealth manager/financial advisor.


22 These three stages of the money laundering cycle are usually referred to as placement, layering and integration, United Nations Office on Drugs and Crime, The Money Laundering Cycle (http://www.unodc.org/unodc/en/money-laundering/laundrycycle.html)
funds and/or actors. This validation will also provide assurances to the institution that the SARs are regulatory sufficient.

**A “Four Corners” Approach**

In essence, what is reported in the narrative becomes the SAR’s dictating canon. By utilizing the four corners of the narrative, an auditor can determine how well the institution’s AML program is working.

The narrative should contain all of the material information from the case file and/or investigative diary and the inverse should hold true as well. By relying on the narrative as a mapping tool, an auditor could then retrace the investigator’s decision on why a SAR was appropriate based on the alert and KYC, and cross reference to ensure that the supporting documentation reflects the same. As previously noted, information is frequently referenced in a narrative but the source of that information is absent from the case file or system of record. Validating the SAR’s source documentation against the narrative assists the auditor in determining how consistent those investigators are in deciding whether a SAR was appropriate and in completing the more administrative tasks related to SAR filing. Moreover, that documentation is arguably forensic evidence, which is crucial to law enforcement to retrace the illicit actor’s steps. Given that imperative, an auditor should be able to retrieve that supporting documentation as readily as the institution should be able to furnish it. The absence of materials, which are referenced in the SAR narrative (surveillance footage, signature cards, statements, etc.) should result in a high-risk finding, as they cannot then be validated as reported. Moreover, they can aid the auditor in determining if there is a systemic procedural issue when it comes to how investigators are documenting their cases and SAR decisions.

The four corners of the narrative should also be able to tell an auditor the circumstances under which a transaction monitoring alert was generated, and from there, what “red flags” of the client’s activity triggered that red flag. The narrative’s description of those red flags will reflect two key controls: KYC and training. KYC strength can be determined by how the narrative describes the red flags in a subjective context, meaning why the identified activity is unusual for that specific client. Well-vetted and continually re-reviewed clients will have known patterns of activity. Therefore, the narrative’s description of anomalous transactions will be reflective of how well the institution knows their customer.

---

23 “Red Flags” refer to potential suspicious activity that “may help banks and examiners recognize possible money laundering and terrorist financing schemes.” FFIEC BSA/AML Examination Manual, Appendix F
Training, as a key control, is demonstrated by understanding why the alerts are relevant to the client and being able to discern them into a reportable offense.\textsuperscript{24} As an example, in the 2014 JPMC Deferred Prosecution Agreement, the statement of facts indicates that only two transaction monitoring alerts were generated on the Madoff Securities account. One of those alerts was raised because the account at issue received $757.2 million in electronic transfers, which was 2,700 percent higher than the past 90 days of activity. This alert (along with the other) was closed out with no SAR issued because the activity was deemed to be “usual” for the relationship, despite the absence of refreshed KYC information.\textsuperscript{25} Arguably, had the KYC information been up-to-date and the investigator’s training more robust (another call out from the deferred prosecution agreement), a SAR could have been filed timely, which indicated why this activity was so subjectively unusual for the client’s relationship.

Both of those questions are well within the purview of a SAR audit and strongly determinative of the overall functionality of a financial institution’s KYC function\textsuperscript{26} as it fits within the larger AML program.

\textbf{IV. Supporting Documentation}

While it seems like a relatively simplistic point to state that the underlying documentation for a SAR must be present, very frequently portions or even the entirety of that documentation is in fact notably absent from an investigative case file. According to U.S. guidance, banks must have and retain the SAR-pertinent documentation for a period of five years from SAR filing, and this documentation can be in paper or electronic format. The purpose for having this supporting documentation on hand is so that law enforcement can be furnished “all documents or records that assisted a bank in making the determination that certain activity required a SAR filing.”\textsuperscript{27} Beyond being a requirement, the absence, presence and quality of the supporting documentation has a two-fold benefit to an auditor examining SARs (or the entirety of a FCC program). First, that documentation can be utilized to thoroughly assess how the SAR issuer came to the decision to file and where they derived the information populated in the form and narrative. The guidance broadly states “all documents or records,” which can be read to include the bank’s own system of record, external databases, as well as information that the SAR issuer comes to learn during the course of an investigation.

\textsuperscript{24} USA PATRIOT Act, Title III, Section 352
\textsuperscript{25} JP Morgan Chase Bank, N.A. Deferred Prosecution Agreement, Exhibit C, Statement of Facts, Page 5, Section 21
\textsuperscript{26} “Banks should not only establish the identity of their customers, but should also monitor account activity to determine those transactions that do not conform with the normal or expected transactions for that customer or type of account.” Customer Due Diligence For Banks, Essential Elements of KYC Standards, Page 5, Section 19, Basel Committee On Supervision, October 2001
\textsuperscript{27} FFIEC BSA/AML Examination Manual, Page 73, Record Retention and Supporting Documentation
investigation. From a functional perspective, the auditor should be able to ‘pick up’ a SAR and retrace all sources of information in the form and narrative.\textsuperscript{28} For example, it may not be unusual for a bank’s investigative staff to liaise with law enforcement during the course of an investigation and to receive information on the subject of that investigation. When that is the case, if the information (true name, date of birth, additional identifiers, etc.) is referenced in the SAR but did not come from an additionally documented record, the law enforcement referral must be noted so that there are auditable sources of that information.

Second, the quality of the documentation can aid the auditor in determining how consistently a team leader or manager is driving the need for that underlying documentation. Where there are consistent gaps in the documentation by one SAR issuer then that speaks to a coaching or performance issue for that individual. However, if numerous SAR issuers under one management team present discrepancies in the type of documentation they are purportedly relying on in order to make the determination to file a SAR, then that speaks to a management oversight issue. This could be symptomatic of a lack of onboarding or continuing education, where SAR issuers are relying on misinformed peers for guidance instead of a uniform set of guidelines, or where there is no institutional tone from the top reflecting the need for consistency in the AML program. As an auditor, the next logical step to is to examine what the relevant functional instructional manual (FIM) dictates, and how management trains to that. Again, a related finding could be that the FIM itself is vague, out-of-date, or otherwise inappropriate for that group. Inconsistent documentation standards or execution can expose the institution to regulatory scrutiny, but more gravely, can affect the quality of law enforcement’s investigation if SAR information appears to be based off of supposition as opposed to an auditable source.

V. SAR Filing Process, Quality Assurance and Quality Control

Guidance surrounding SAR completion and filing in general broadly dictates whether the bank’s FIMs provide for filing, reporting SAR trends upwards, and whether the decision process is completed and SARs are filed in a timely manner.\textsuperscript{29} Absent precise language from an enforcement action or updated guidance, there is very little guidance on the Quality Assurance (QA) process to give institutions an idea of what an optimum program should look like. Many institutions have already turned to a sort of “tollgate” process where, despite the 30-day timeline, SARs must be generated and complete by

\textsuperscript{28} Id.
\textsuperscript{29} FFIEC BSA/AML Examination Manual Examination Procedures, Page 78, Section 15; FFIEC BSA/AML Examination Manual, Page 79, Section 23
calendar day 20 or 25, for example. In the remainder of the 30-day window, the institution carries out a QA process on the SARs prior to the reports being formally ‘issued.’ For an auditor in an institution that relies on this type of process, this QA window can deliver a harvest of findings relevant to the institution’s AML program.

**The QA Process**

For the auditor, if a QA tollgate is included in the SAR process then an audit of that process must include two key aspects: subjective and objective outcomes. The findings on a case-by-case basis (subjective outcomes) include typos, miscategorizations of activity, and other substantive failures. Subjective outcomes are indicative of an individual SAR filer or team of SAR filers’ lack of training, staffing, or resources to file a SAR. The objective outcomes are the sum of the QA effort, meaning what recommendations if any are the QA processors coming up with based on a holistic review of the subjective outcomes. The objective outcomes should be able to indicate larger steering issues in the SARs and, if the subjective outcomes have a low error rate, help the institution to determine trends in suspicious activity. Whether or not the QA process specifically produces objective and subjective outcomes is not necessarily as relevant as what deliverables arise from the outcomes. Anecdotally, many institutions use the QA process to ‘grade’ the SARs or the SAR filers but take no corrective action to train the erroneous SAR filer based on that grade. Or, the QA process will result in a tally of overall qualitative errors, but those errors are not analyzed or used to drive change going forward. For an auditor, these QA outcomes should at the very least be included in management information (MI). Optimally, there should also be some documented progression that reflects the root causes for subjective/objective outcome and from there, action plans or management directives should be generated which indicate what the ‘next steps’ are in rectifying these issues throughout the institution’s SAR filing footprint.

**Defensive SAR Filings**

Defensive filings, where an institution files a report simply to “[avoid] regulatory and criminal scrutiny under the Bank Secrecy Act is to file more reports, regardless of whether the conduct or transaction identified is suspicious” are not at all a new phenomenon.\(^3^0\) Defensive filings generally do not add value to law enforcement or the institution’s program itself, and may even “degrade the valuable reports in the database and implicate privacy concerns.”\(^3^1\) Again, institutions should, to the best of their ability, identify the

---

\(^{30}\) The SAR Activity Review, Trends Tips & Issues, Section 1, Page 3, FinCEN, 2005  
\(^{31}\) Id.
characteristics of the suspicious activity” and any sample of SARs should sufficiently reflect that those characteristics and the thresholds needed for filing have been met. If the auditor cannot identify that the basic criteria were met and confirmed by the SAR filer and QA staff respectively, then it could be inferred that both areas of the institution have not received sufficient, relevant AML training.

**Auditing the No-SAR Scenario**

With the increase in regulatory scrutiny that financial institutions have faced over the past five to 10 years, many institutions likely take the decision not to file a SAR more seriously than the determination to actually issue a report. For the auditor, examining a no-SAR scenario can and should be the capstone in the SAR audit. The no-SAR should entail of the key benchmarks of a quality AML program, which would be reflected in an audit of the workflow of the alert. A hypothetical QA workflow is below with audit considerations:

**First Consideration – Monitoring** – Was the alert that was generated appropriate for that client, or was it a generic alert which frequently yields no-SARs for this or numerous other clients? Have there been numerous alerts for this client or is this the first one and what is the type of alert? For example, if it is a threshold level alert on a private banking client, but the monitoring rule’s dollar amount or account balance ratio was for a run-of-the-mill limit retail customer, then the rule for that customer and perhaps all similar customers is inappropriate.

**Second Consideration – KYC** – If the alert was in fact sufficiently tailored to this client typology, was there sufficient KYC completed on the customer for the SAR filer to be able to put the alert into context? For example, does the client’s KYC information clearly indicate the client’s contemporaneous sources of wealth and funds so that the SAR filer can determine what is normal for this client? Are there gaps in the documentation that leave the filer unable to make a strong determination of the client’s AML risk in conjunction with the alert? From there, would the SAR decision-maker/QA processor know enough to understand that those gaps are the reason for a no-SAR?

---

32 FFIEC BSA/AML Examination Manual Examination Procedures, Pages 67-68, Identifying Underlying Crime  
33 A “No-SAR” scenario generally refers to an instance where a transaction monitoring alert was raised but, after a review of the activity, no alert was generated.  
34 Nearly U.S.$5 billion in monetary penalties against financial institutions in connection with alleged violations of BSA/AML regulations since 2007 and two-thirds of all formal enforcement actions since 2012 have included monetary penalties, compared to only one-third from 2007 through 2011 – “Recent Trends in BSA/AML Enforcement and Litigation”, NERA Economic Consulting, Date Unknown
**Third Consideration – Threshold** – What transactions are the SAR filer basing their threshold accumulation? The requisite threshold should be based on any transaction(s) reaching $5,000 or $25,000 (or other amounts where regulatory required), and given the diversity of money laundering techniques, should include activity that appears to be related to the underlying alert-generating transaction. For example, in an account indicative of smurfing activity, the individual transactions may be a wire, party to party transfer, cash deposit, or merchant processing. Although diverse transactions may not reach the requisite threshold individually, the savvy SAR filer must understand that a transaction (in the U.S.) is meant to include a broad array of banking activities. If an auditor can identify additional unusual activity that could have merited the SAR filer issuing a report, then the root cause of the failure to file is a lack of training at the individual or management level.

**Fourth Consideration – Decision-making** – Can an auditor review a case file and readily validate that the no-SAR was appropriate? This should be evidenced in the case documentation and, where available, in the case journal. Validation, in this instance, is correlative to the auditor arriving at the same conclusion as the SAR filer. In a best case scenario, the documentation would speak for itself and the auditor would not need to interview the individual filer to better understand the decision. Moreover, the auditor should be able to readily view that there is not only a SAR/no-SAR decision-making procedure for filers to follow, but that all no-SARs in the sample met that process. Higher risk findings might present as no-SAR decisions where the alert is simply ‘moved’ to the no-SAR stage and approved without documentation to support why, or that the no-SAR decision was approved/advised by another party without identifying those persons. SAR auditors should be satisfied if the institution has a step-by-step process which is adhered to closely. This process should indicate the steps for no-SAR approval, includes SAR timeliness as a reference point and a traceable mechanism for escalating debates over whether or not to file. Conversely, an auditor should be very concerned over a SAR filer who has complete autonomous authority to close an alert with no supervisory checks.

---

35 “Smurfing” or structuring is defined as depositing cash at various institutions in amounts less that the amount that must be reported to government, and subsequently transferring them to a central account. New Zealand Ministry of Justice, Money Laundering and Terrorism Financing (http://www.justice.govt.nz/policy/criminal-justice/aml-cft/money-laundering-and-terrorism-financing)

36 “A transaction includes a deposit; a withdrawal; a transfer between accounts; an exchange of currency; an extension of credit; a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security; or any other payment, transfer, or delivery by, through, or to a bank.” FFIEC BSA/AML Examination Manual, Suspicious Activity Reporting Overview, Page 60-61
In the end, SAR/no-SAR decision-making is the most challenging facet of the AML program to audit because, even in the face of sufficient monitoring and KYC, it comes down to a SAR filer’s judgment. That judgment, of course, can only be finely tuned based on the availability of staffing to cover the number of alerts generated as well as how well that staff has been trained. Take again, for example, the JPMorgan Chase (JPM) enforcement action. In regards to the contested account, the statement of facts indicates that despite two transaction alert being generated on the Madoff Securities account, “[i]n both cases, the AML investigators closed the alerts with a notation that the transaction did not appear to be unusual for the account’s prior activity.”37 Assuming all of the requisite information was present and the threshold had been met, the auditor’s question would be whether or not the SAR filer was sufficiently trained to 1) know what a “Ponzi” type investment fraud scheme looks like in a client account and 2) understood that they should have also questioned whether the account activity was comparable to other similar types of customers (i.e., subjectively normal for Madoff Securities but objectively unusual for other investment advisory firms). These types of no-SAR decision-making errors are based on training and management failures and, as with JPM, can be strong indicators of more systemic AML program failures.

VI. Conclusion

A SAR is a derivative product of three of the four pillars:38 policies, procedures and controls such as KYC and monitoring, training and designated AML staff. A well-executed SAR will contain concise information about what the institution suspects their client(s) did, what triggered the review on the customer that led the institution to that conclusion and the illicit customer’s known information.

Accordingly, validating the source information of a SAR through the lens of both the SAR’s functional and regulatory purposes can only serve to insulate an institution against programmatic pillar failures. Therefore, auditing (the fourth pillar) the SAR as a diagnostic tool for those underlying operative AML pillars can definitively serve to map the key controls’ strengths and deficiencies throughout an institution’s AML program.

37 JP Morgan Chase Bank, N.A. Deferred Prosecution Agreement, Exhibit C, Statement of Facts, Page 5, Section 21
38 USA PATRIOT Act, Title III, Section 352
References

2. FFIEC BSA/AML Examination Manual Examination Procedures, Pages 67-68, Identifying Underlying Crime
3. FFIEC Bank Secrecy Act/Anti-Money Laundering Examination Manual, Page 68, SAR Filing on Continuing Activity
5. JPMorgan Chase Bank, N.A. Deferred Prosecution Agreement, Exhibit C, Statement of Facts, Page 5, Section 21; Page 19, Section 85
7. FinCEN Advisory to U.S. Financial Institutions on Promoting a Culture of Compliance, FIN-2014-A007, August 11, 2014
8. SAR Data Quality Requires FinCEN’s Continued Attention, Pages 12-13, Office of the Inspector General, Department of the Treasury, January 19,2010, OIG-10-030
10. SAR Data Quality Requires FinCEN’s Continued Attention, Pages 17, Office of the Inspector General, Department of the Treasury, January 19,2010, OIG-10-030
11. FFIEC BSA/AML Examination Manual Examination Procedures, Page 69, SAR Completion and Filing
12. New York State Law, Penal Law, Part 3, Title K, Article 190.00-190.1
15. FFIEC BSA/AML Examination Manual Appendix F
17. FFIEC BSA/AML Examination Manual, Page 73, Record Retention and Supporting Documentation
18. FFIEC BSA/AML Examination Manual Examination Procedures, Page 78, Section 15;
19. FFIEC BSA/AML Examination Manual, Page 79, Section 23
20. The SAR Activity Review, Trends Tips & Issues, Section 1, Page 3, FinCEN, 2005
21. “Recent Trends in BSA/AML Enforcement and Litigation”, NERA Economic Consulting, Date Unknown
23. FFIEC BSA/AML Examination Manual, Suspicious Activity Reporting Overview, Page 60-61