Examination Procedures

Suspicious Activity Reporting

Objective. *Assess the bank’s policies, procedures, and processes, and overall compliance with statutory and regulatory requirements for monitoring, detecting, and reporting suspicious activities.*

| **Procedure** | **Comments** |
| --- | --- |
| Initially, examiners may elect to “map out” the process the bank follows to monitor for, identify, research, and report suspicious activities. Once the examiner has an understanding of the process, the examiner should follow an alert through the entire process. | |
| **Identification of Unusual Activity** | |
| 1. Review the bank’s policies, procedures, and processes for identifying, researching, and reporting suspicious activity. Determine whether they include the following:  * Lines of communication for the referral of unusual activity to appropriate personnel. * Designation of individual(s) responsible for identifying, researching, and reporting suspicious activities. * Monitoring systems used to identify unusual activity. * Procedures for reviewing and evaluating the transaction activity of subjects included in law enforcement requests (e.g., grand jury subpoenas, section 314(a) requests, or National Security Letters (NSLs)) for suspicious activity. NSLs are highly confidential documents; as such, examiners will not review or sample specific NSLs. Instead, examiners should evaluate the policies, procedures, and processes for: * Responding to NSLs. * Evaluating the account of the target for suspicious activity. * Filing SARs, if necessary. * Handling account closures. |  |
| 1. Review the bank’s monitoring systems and how the system(s) fits into the bank’s overall suspicious activity monitoring and reporting process. Complete the appropriate examination procedures that follow. When evaluating the effectiveness of the bank’s monitoring systems, examiners should consider the bank’s overall risk profile (higher-risk products, services, customers, entities, and geographic locations), volume of transactions, and adequacy of staffing. |  |
| **Transaction (Manual Transaction) Monitoring** | |
| 1. Review the bank’s transaction monitoring reports. Determine whether the reports capture all areas that pose money laundering and terrorist financing risks. Examples of these reports include: currency activity reports, funds transfer reports, monetary instrument sales reports, ATM transaction reports, large item reports, significant balance change reports, nonsufficient funds (NSF) reports, and nonresident alien (NRA) reports. |  |
| 1. Determine whether the bank’s transaction monitoring systems use reasonable filtering criteria whose programming has been independently verified. Determine whether the monitoring systems generate accurate reports at a reasonable frequency. |  |
| **Surveillance (Automated Accounting) Monitoring** | |
| 1. Identify the types of customers, products, and services that are included within the surveillance monitoring system. |  |
| 1. Identify the system’s methodology for establishing and applying expected activity or profile filtering criteria and for generating monitoring reports. Determine whether the system’s filtering criteria are reasonable. |  |
| 1. Determine whether the programming of the methodology has been independently validated. |  |
| 1. Determine that controls ensure limited access to the monitoring system and sufficient oversight of assumption changes. |  |
| **Managing Alerts** | |
| 1. Determine whether the bank has policies, procedures, and processes to ensure the timely generation of, review of, and response to reports used to identify unusual activities. |  |
| 1. Determine whether policies, procedures, and processes require appropriate research when monitoring reports identify unusual activity. |  |
| 1. Evaluate the bank’s policies, procedures, and processes for referring unusual activity from all business lines to the personnel or department responsible for evaluating unusual activity. The process should ensure that all applicable information (e.g., criminal subpoenas, NSLs, and section 314(a) requests) is effectively evaluated. |  |
| 1. Verify that staffing levels are sufficient to review reports and alerts and investigate items, and that staff possess the requisite experience level and proper investigatory tools. The volume of system alerts and investigations should not be tailored solely to meet existing staffing levels. |  |
| 1. Determine whether the bank’s SAR decision process appropriately considers all available CDD and EDD information. |  |
| **SAR Decision Making** | |
| 1. Determine whether the bank’s policies, procedures, and processes include procedures for:  * Documenting decisions not to file a SAR. * Escalating issues identified as the result of repeat SAR filings on accounts. * Considering closing accounts as a result of continuous suspicious activity. |  |
| **SAR Completion and Filing** | |
| 15. Determine whether the bank’s policies, procedures, and processes provide for:   * Completing, filing, and retaining SARs and their supporting documentation. * Reporting SARs to the board of directors, or a committee thereof, and informing senior management. * Sharing SARs with head offices and controlling companies, as necessary. |  |
| **Transaction Testing** | |
| Transaction testing of suspicious activity monitoring systems and reporting processes is intended to determine whether the bank’s policies, procedures, and processes are adequate and effectively implemented. Examiners should document the factors they used to select samples and should maintain a list of the accounts sampled. The size and the sample should be based on the following:   * Weaknesses in the account monitoring systems. * The bank’s overall BSA/AML risk profile (e.g., number and type of higher-risk products, services, customers, entities, and geographies). * Quality and extent of review by audit or independent parties. * Prior examination findings. * Recent mergers, acquisitions, or other significant organizational changes. * Conclusions or questions from the review of the bank’s SARs.   Refer to Appendix O in the manual (“Examiner Tools for Transaction Testing”) for additional guidance. | |
| 1. On the basis of a risk assessment, prior examination reports, and a review of the bank’s audit findings, sample specific customer accounts to review the following:  * Suspicious activity monitoring reports. * CTR download information. * Higher-risk banking operations (products, services, customers, entities, and geographies). * Customer activity. * Subpoenas received by the bank. * Decisions not to file a SAR. |  |
| 1. For the customers selected previously, obtain the following information, if applicable:  * CIP and account-opening documentation. * CDD documentation. * Two to three months of account statements covering the total customer relationship and showing all transactions. * Sample items posted against the account (e.g., copies of checks deposited and written, debit or credit tickets, and funds transfer beneficiaries and originators). * Other relevant information, such as loan files and correspondence. |  |
| 1. Review the selected accounts for unusual activity. If the examiner identifies unusual activity, review customer information for indications that the activity is typical for the customer (i.e., the sort of activity in which the customer is normally expected to engage). When reviewing for unusual activity, consider the following:  * For individual customers, whether the activity is consistent with CDD information (e.g., occupation, expected account activity, and sources of funds and wealth). * For business customers, whether the activity is consistent with CDD information (e.g., type of business, size, location, and target market). |  |
| 1. Determine whether the transaction or surveillance suspicious activity monitoring system detected the activity that the examiner identified as unusual. |  |
| 1. For transactions identified as unusual, discuss the transactions with management. Determine whether the account officer demonstrates knowledge of the customer and the unusual transactions. After examining the available facts, determine whether management knows of a reasonable explanation for the transactions. |  |
| 1. Determine whether the bank has failed to identify any reportable suspicious activity. |  |
| 1. From the results of the sample, determine whether the transaction or surveillance suspicious activity monitoring system effectively detects unusual or suspicious activity. Identify the underlying cause of any deficiencies in the monitoring systems (e.g., inappropriate filters, insufficient risk assessment, or inadequate decision-making). |  |
| 1. On the basis of a risk assessment, prior examination reports, and a review of the bank’s audit findings, select a sample of management’s research decisions to determine the following:  * Whether management decisions to file or not file a SAR are supported and reasonable. * Whether documentation is adequate. * Whether the decision process is completed and SARs are filed in a timely manner. |  |
| 1. On the basis of a risk assessment, prior examination reports, and a review of the bank’s audit findings, sample the SARs downloaded from the BSA reporting database or the bank’s internal SAR records. Review the quality of SAR content to assess the following:  * SARs contain accurate information. * SAR narratives are complete and thorough, and clearly explain why the activity is suspicious (i.e., the SAR narrative should not simply state “see attachment” if the bank included a csv file). |  |
| 1. On the basis of examination procedures completed, including transaction testing, form a conclusion about the ability of policies, procedures, and processes to meet regulatory requirements associated with monitoring, detecting, and reporting suspicious activity. |  |