

# Suspicious Activity Investigation Lifecycle

An alert has occurred! How do I know if it's a legitimate problem? Knowing when to trip the alarm and investigate can be a daunting task for any organization with an Anti-Money Laundering Program. Understanding each step, utilizing opportunities for technology and automation, as well as having a great staff that know the signs of suspicious activity can help your organization protect itself and "hear through the noise." Remember that your focus is to identify suspicious activity and report it, not to prove criminality; law enforcement will take it from there, blending your information with information from other institutions before making a decision on how to proceed.

## TRIAGE

Understanding and managing your inbound alerts can be an intimidating task. High alert volume and false-positives can abound, often at a 50:1 ratio (False/True). Focus on automated solutions that allow you to invest human capital into exception cases. Consistently review and modify the system until your organization can hear through the noise.

## INVESTIGATION

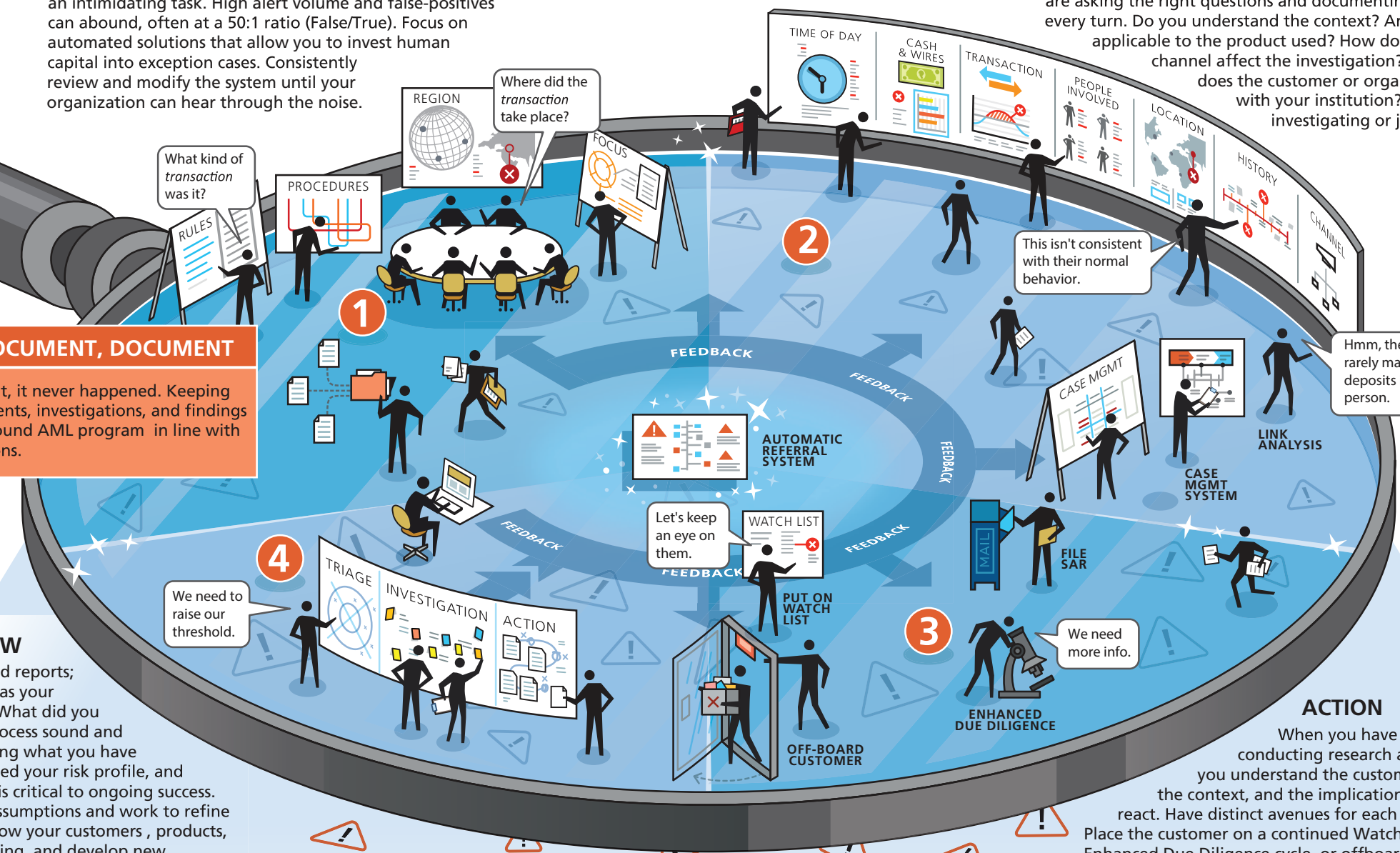
The Investigation process can tax your resources. Make sure you are asking the right questions and documenting the process at every turn. Do you understand the context? Are your procedures applicable to the product used? How does the processing channel affect the investigation? What history does the customer or organization have with your institution? Are you truly investigating or just documenting?

## DOCUMENT, DOCUMENT, DOCUMENT

If you don't document, it never happened. Keeping close records of incidents, investigations, and findings are imperative to a sound AML program in line with regulatory expectations.

## FEEDBACK/REVIEW

Review your actions and reports; were they accurate? Was your investigation fruitful? What did you learn? Is our current process sound and comprehensive? Learning what you have done, how it has affected your risk profile, and how you have reacted is critical to ongoing success. Constantly challenge assumptions and work to refine the process. Evaluate how your customers, products, and business are changing, and develop new scenarios.



## BEST PRACTICES

- Constantly challenge the current assumptions and evaluate the soundness of your program
- Regularly review and adjust thresholds and consider new typologies
- Send inquiries when appropriate
- Institute a culture of compliance-ensure the staff is aware and empowered to do the right thing
- Conduct ongoing monitoring and outcome analysis
- Train continually

## COMMON MISTAKES

- Lack of documentation
- Missing internal and external deadlines
- Poor quality, incomplete, or overly vague Suspicious Activity Reports
- Tipping off customer during the inquiry process
- Sending inquiries that contain vague or misleading questions
- Setting the bar for suspicious activity too high, causing an overwhelming number of false-positive alerts
- Not tuning the system based on lessons learned

## TECHNOLOGY

Tools are available at every stage of the Anti-Money Laundering Investigation Lifecycle. Understanding how they can minimize your human capital commitment as well as increase your positive case discovery is critical. Current technology tools can include:

- Automated Referral Systems
- Case Management Systems
- Link Analysis
- Quality Control
- Governance Processes
- Tuning and Optimization