



Levelling up: A practical guide to sanctions investigations for FIs



An understanding of what's involved in an investigation for potential sanctions violations is a critical component to a well-functioning compliance programme for FIs and non-FI corporations alike, argues **Mark Struth**, who sets out the options, and explores best practice.

Financial institutions have a clear obligation to prevent sanctions breaches and identify them where they occur. They achieve this through the implementation of controls to detect and prevent activity that may have a sanctions nexus, using tools such as transaction screening, customer due diligence and transactional activity. The controls implemented are in line with the firm's risk-based approach which, in turn, is dependent on the nature, size and complexity of the firm and its operations. As such, the implementation of these controls varies.

Sanctions detection activity alerts the FI that there may be a sanctions nexus to the activity in question. The FI needs to review this activity to determine the extent of a possible nexus and to determine the appropriate course of action. Usually, specialist teams will be prevailed upon to undertake the investigation.

STAGES OF AN INVESTIGATION

There are three stages to any sanctions investigation:

1. Identification
2. Assessment
3. Decision and next steps

It is common for the stages in the investigation to be split between several teams depending on the size and the complexity of the FI. For example, payment screening investigations may be split over three teams (three-level investigations), though some firms may take a one-level approach, and others up to five – the discrepancy accounted for by varying products, systems, operating structures and detection systems. In practice, three-level investigations are the most common.

Identification of sanctions issues

The first stage of the investigation relates to the identification of a potential

sanctions nexus to activity. This can range from utilising bespoke detection tools, such as payment and customer screening, to ad-hoc referrals from internal colleagues within the firm. If a sanctions nexus is determined, it is escalated to an investigation team to start the review. The frequency of sanctions escalations and sources vary in line with business operations.

Broadly, there are two types of sanctions escalation within the FI – structured and unstructured.

Structured escalations are system-generated, usually from detection systems such as payment and account screening and case management portals. If there is a structured escalation, there will usually be a structured process to follow.

This provides the investigation teams with the advantage of an inbuilt audit trail and workflow,

and contains information pertinent to the investigation within the escalation, and even enforcement of systemic controls such as holding payment messages, until such time as the investigation is complete. This is useful as it can speed up investigations, decreasing the time spent on finding information and directing business teams to hold/release payments. This time can be spent focusing on resolving the investigation itself.

Structured investigations also have disadvantages, with inherent inflexibility and systemic constraints such as an enforced workflow. They can be complex to use and can be limited in the amount and type of information that can initially be provided to the investigators. They can also be limited to the narrow scope of the detection tool/system they review. Structured escalations are usually best suited for high-volume events (payments and account-screening escalations).



IT IS IMPORTANT THAT THE INVESTIGATORS UNDERSTAND THE SOURCE OF THE SANCTIONS CONCERN, THE END-TO-END PROCESS SUPPORTING THE ESCALATION, AND THE DETECTION TOOL OR AREA THAT IS ESCALATING.

Unstructured escalations are usually where there is absence of a systems-based escalation, and the escalation has been sent by a person.

This is usually where a sanctions concern has been determined through the course of usual business, but there is not enough perceived risk or volume for a systemic control to be considered viable. For instance, AML teams reviewing suspicious activity reports ('SARs') may, through the course of their investigations, determine a sanctions nexus, or front-line staff may have a potential customer concern. Escalations like this can take the form of secure portal or even email. They are unstructured as the escalation content is dependent on the person escalating, they are usually written free-hand and with a lack of a structured content, i.e., someone may simply write a quick sentence to escalate where others may write a detailed precise escalation containing supporting information. It is entirely dependent on the person escalating the concern.

If the escalation is unstructured, there will be difficulties ensuring that the right audit trail is established. Escalations are usually sent directly to compliance teams. However, escalation forms/templates can assist in this scenario. Whilst they may

be difficult to administer and control, unstructured escalations are also valuable sources of intelligence, and they can identify weaknesses in systemic detection tools or connect missing parts to an existing investigation.

It is important that the investigators understand the source of the sanctions concern, the end-to-end process supporting the escalation, and the detection tool or area that is escalating. This is important as steps can be lost, the audit trail can be missed, and information relied upon may turn out to be assumption, not fact, and can thus lead to some significant issues. It is also important to remember that most sanctions teams, particularly at the latter stages of an investigation, have a multitude of different sources and systems to contend with, making management of an investigation workflow difficult and time consuming.

Investigation

After the sanctions concern has been identified and escalated, it needs to be investigated further to confirm that the concern is valid, determine the extent and potential impact of the sanctions nexus, and determine the next steps.

This can be a complex process, and teams are usually under significant business pressure. For

instance, during a payment investigation, payment message/funds are held until a final determination can be made. This is the source of significant tension between the FI and its clients. As such, FIs implement operational strategies for reducing the impact of sanctions investigations on day-to-day operations. The most common of these is the introduction of levels/stages of investigations to filter out the volume of non-genuine concerns at lower levels, focusing and SME's resources on only genuine concerns.

EXAMPLE INVESTIGATION FLOW

Note the operating models and terms used will vary between FIs, the following is a generic example of the most commonly used.

Stage 1: False positive identification

Performed by – Dedicated staff within operations, usually part of payment operations.

Aim – Rule out any obvious false positives (not actual sanctions concerns) that have been generated due to (1) loose matching, (2) common terms/names, (3) list configuration issues or any other issue. They can close false positives. Those that look genuine or inconclusive are escalated to a higher level.

How do they do this? – Rules based/script-based determinations, within a narrow range of acceptable scenarios. (The scenarios are usually reviewed/approved by risk/compliance.)

Output – Cases are closed as confirmed false positives or escalated for further investigation if inconclusive or looks to be a true sanctions concern.

Characteristics of these teams – Highly operational, usually within payment teams, focused on tight deadlines, these teams usually have very

short timescales, (same-day turnaround). With no access to specialist tools to assist, their investigation is limited to the pre-determined script/decision matrix. Lower sanctions subject matter expertise required to perform the role. No customer contact/outreach for more information is required. Anything that requires an additional review is escalated to the next level.

Why not optimise the system and negate the need for these teams? This is possible and does occur, however, this level deals with temporary high volumes whilst the system is optimised. It is important that new topologies are tested, and/or system issues are identified at this level. It is also at this level that individuals and/or entities listed without adequate additional identifiers should be identified. Finally, optimisation for certain scenarios beyond the firm's risk appetite (system capability limits) should be established.

Stage 2: Positive determination

Performed by – First line of defence compliance/investigations team situated within the business operation.

Aim – Confirm that there is a sanctions nexus within the escalation from the previous level

How do they do this? – Performance of a risk-based investigation, determining what key pieces of information are required to determine if there is a true sanctions concern or otherwise. Use of additional internal and third-party sources of data (including Open Source data), internal intelligence data and reaching out to clients to get additional information. Then a decision can be made on the totality of this information.



THE RISK FOR THE TEAM IS THAT THE PRESSURE CAN LEAD TO INVESTIGATOR ERROR.

Output – Depending on the outcome of the investigation, if the team determine there is a genuine sanctions concern, they will escalate for a final review and action to compliance/legal.

The team will also escalate where it cannot be determined either way and there is enough to indicate a sanctions nexus. If there is a false positive this will be resolved by the team.

Certain positive determinations may be permitted, allowing Stage 3 to take action where the activity has been pre-determined to be permissible, and this is a repeat transaction, though this should be temporary (whilst a systemic solution is implemented) and requires the risk owner to authorise this approach.

The reasons for the escalation or closure will be detailed, and evidence supporting the decision will be contained in the escalation.

Characteristics of the team – These are a hybrid between operational and investigation teams, as they need to understand the operational processes surrounding the transactions or on-boarding processes. They can use this experience to determine the likelihood of receiving additional information. Sanctions subject matter expertise is also required to understand the applicability of any authorisations that the Stage 3 teams provide

for certain activity that is deemed permissible.

Typically, the middle team in the process, they also co-ordinate and deal with actions such as blocking/freezing funds and giving updates to internal stakeholders on the progress of investigations.

Stage 3 – Determine the impact and next steps

Performed by – Second line of defence, compliance or legal teams. Non-operational teams, usually subject matter experts in both sanctions and how they apply to the products and services that the FI offers.

Aim – Review the extent to which the sanctions apply to the activity in question, determine the next steps for the FI.

How do they do this?
– A review of the facts pertaining to the case, determining the extent to which a programme extends to the transaction/business activity in question. For instance, does it fall within the territorial scope of the sanctions in question? Is the underlying activity out of scope of prohibitions/restrictive measures? Is it actually permissible under a general licence or exemption? Is the activity itself not within the scope of sectoral sanctions (i.e., payments in respect of goods/services for EU Russia Sectoral Sanctions)?

They will also identify and review potential conflicts in local law with the extraterritoriality of certain sanctions regimes and, co-ordinating with other areas of the FI such as operational and reputational risk teams, internal/external legal counsel as required in order to determine the appropriate course of action. Additional information may be requested from the business if it helps the determination.

Output – If deemed

permissible, the case will be updated, and the business will be advised to allow the activity to proceed (follow-on activity will review with Stages 1 and 2 to prevent false escalations.)

If not permissible:

- The payment will need to be either frozen/blocked (EU/US) or cancelled, depending on the sanctions programme. In this case, the team will make the request to Stage 2 teams to take appropriate action and provide evidence that action has been taken.
- Reporting obligations to the issuing authority are determined and co-ordinated by the team (though certain FIs use internal legal counsel, depending on operating model). The evidence of reporting is required for record keeping. In addition, the team may deal with follow-up requests from the issuing authorities.

In addition for all cases:

Remediation and risk reduction activity – The root cause of the sanctions concern will be reviewed to determine if there are follow on actions, such as updating risk and threat assessments, detection improvements (screening rules update) or highlighting operational control improvements within the business.

Characteristics of the team – Subject matter experts on sanctions and how they apply specifically to the products/services and operations of the FI. Typically, smaller teams than the other stages. Usually independent from the operation and are the central source of sanctions escalations throughout the business.

The volume of escalations is lower at this stage, however, the complexity of the cases at this stage leads to the cases taking longer to review.

SANCTIONS INVESTIGATION CHALLENGES

Real-time nature of investigations

Most investigations are real-time, which means that a live payment, deal or account is being assessed, and during the investigation the activity will be held awaiting a determination of next steps. This can lead to:

- Business pressures (constant case update requests).
- Client friction with front-line staff as they are unaware of the reason for the delay.
- Business impact, loss of clients, particularly for deadline driven events (market activity).

The risk for the team is that the pressure can lead to investigator error, trying to adhere to the deadlines. In addition, constant chasers for updates and pressure on the team can lead to stress and burnout, which can lead to high staff attrition rates. This is a significant issue for smaller compliance teams with less operational resilience.

Strategy – Usually the compliance teams will not be directly contactable for business teams, the other teams in the process (Stage 1 & 2) will handle client and business cases.

Investigation systems and tools

Multiple systems – Investigation systems can be fragmented depending on the source of the sanctions investigation. For instance, there can two different systems for account and transaction screening systems, or several different escalation sources.

Tools – Third-party data can be very useful to investigators, for instance access to maritime information, certain owners/controllers of entities and

local intelligence sources. The challenge here is that access to such tools is limited given their relative expense to the FI and the fact that they are not always required, it depends on the escalation. However, the FI will need to pay per person all the time. This makes for a tough business case!

These issues can lead to

- Inefficiency: Multiple systems lead to additional complexity and time taken to review (possible duplication of cases, fragmented oversight and reporting).
- Delays: Usually a smaller number of team members have access to specialist tools – there are delays whilst cases are referred to those team members.
- Risk of missing vital information: Investigators may not have access to information vital to the case and may make assumptions.

Strategy – Focus on investigation source amalgamation and a single case management layer on top of the multiple escalation points. This can take significant time and be limited in effectiveness depending on the size and system complexity of the FI. For the third-party tools, business cases can be made on the most effective/used tools. This takes significant time but can be worth the effort. However, open-source training is also highly valuable, as many teams struggle with effective open-source identification (particularly at Stage 2).

COMPLEXITY

Many FIs have complex systems and processes, and the three-stage investigation process can be performed by different teams, sometimes in different locations and time zones. In addition, the cases that are escalated can be complex in nature with potential conflicts of law, deadlines and business

pressure. This can lead to:

- miscommunication between investigation teams;
- escalation of unnecessary cases between stages – creating delay;
- lack of clear accountability between teams – leading to delays and miscommunication;
- inaccurate information escalated to Stage 3 teams; and
- issues with applying remediation action (blocking/reporting, etc.).

Strategy – Reduce complexity, develop clear investigation strategies for each reporting line, and clear roles and responsibilities. Improve communication and share knowledge.

Subject matter expertise

Given the dynamic nature of sanctions and that businesses are always in flux, (new products/systems/processes), it is critically important that all stages of the investigation are knowledgeable on sanctions and business processes. However, this can be difficult given the multiple pressures on the teams from an operational perspective.

Strategy – Resource teams to take into account the need to train and keep the teams up to date. Develop ongoing training plans with teams. Encourage cross team feedback and sessions to review cases.

CONCLUSION

There are a number of challenges that investigating teams will face in an FI, and potentially many teams will be involved in a decision.

However, it is also worth mentioning that, whilst there may be challenges, it is an exciting and rewarding role within the FI. Critically, they are a valuable resource of knowledge and feedback on the performance of the compliance programme within the firm. After all,



REDUCE COMPLEXITY, DEVELOP CLEAR INVESTIGATION STRATEGIES FOR EACH REPORTING LINE, AND CLEAR ROLES AND RESPONSIBILITIES. IMPROVE COMMUNICATION AND SHARE KNOWLEDGE.

they see the compliance programme in action.

If the investigation teams are built up and looked after, they will usually pay it back many times over in return to the FI as a valuable line of defence against breaching sanctions, and identification of control weakness within the firm. ✓

Mark Struth is a seasoned practitioner of Sanctions investigations within financial institutions, having gained extensive experience of sanctions investigations within complex tier-one banks, such as HSBC and latterly Citibank Europe, where he led the Sanctions Compliance Investigation Function for the EMEA region.