SWIFT Financial Crime Compliance
Info paper

Simplify the complex world of sanctions screening

Context
Effective screening, as part of an overall compliance programme, is a crucial component of an organisation's financial crime toolkit, helping them to meet regulatory and due diligence obligations.

With many correspondent banks opting to terminate relationships in high-risk markets, there is a growing need for local banks to reassure correspondents that they have robust compliance processes in place. So effective screening is more important than ever – but what does this involve in practice?

What do screening activities cover?

Screening provides a powerful defence against illicit financial partners and activities and is essential for transparent and traceable financial crime compliance.

Screening can be carried out against lists, such as:

Sanctions lists	Entities and individuals, including OFAC, United Nations and HMT lists.
Sanctions Ownership Research (SOR)	Entities owned or controlled by sanctioned companies and individuals.
Politically Exposed Persons (PEPs)	Individuals with political exposure that are regarded as being at a higher risk of bribery, corruption and money laundering.
Relatives and Close Associates (RCAs)	People related to or associated with PEPs.
Adverse media	For corporate and high-risk accounts – PEPs, RCAs and high net worth individuals – financial institutions may also need to check for adverse media or negative news coverage.

The objective is to screen data to flag high-risk customers, accounts and transactions. Sanctioned individuals should be prevented from using the financial system, whereas PEPs and RCAs can operate accounts as normal. Though institutions should mark PEP and RCAs as being high risk for activities such as money laundering and may choose to apply more extensive due diligence, depending on their specific policies.

Customer screening vs. transaction screening

What's the difference and why do it?

Transaction screening

Transaction screening is the more surgical of the two exercises and involves the real-time, in-flight detection of names of individuals or entities that are prohibited from using the financial system.

The focus is squarely on screening incoming and outgoing messages against sanctions lists to identify potential threats. It also looks at SOR lists to determine whether the entity sending or receiving a message could be owned or controlled by a sanctioned individual or entity.

If a message generates a true match between an item in a transaction and a sanctioned individual or entity, the institution will need to review the specific sanction to understand what action, if any, is required. This might involve freezing funds or blocking all assets and accounts.

Customer screening

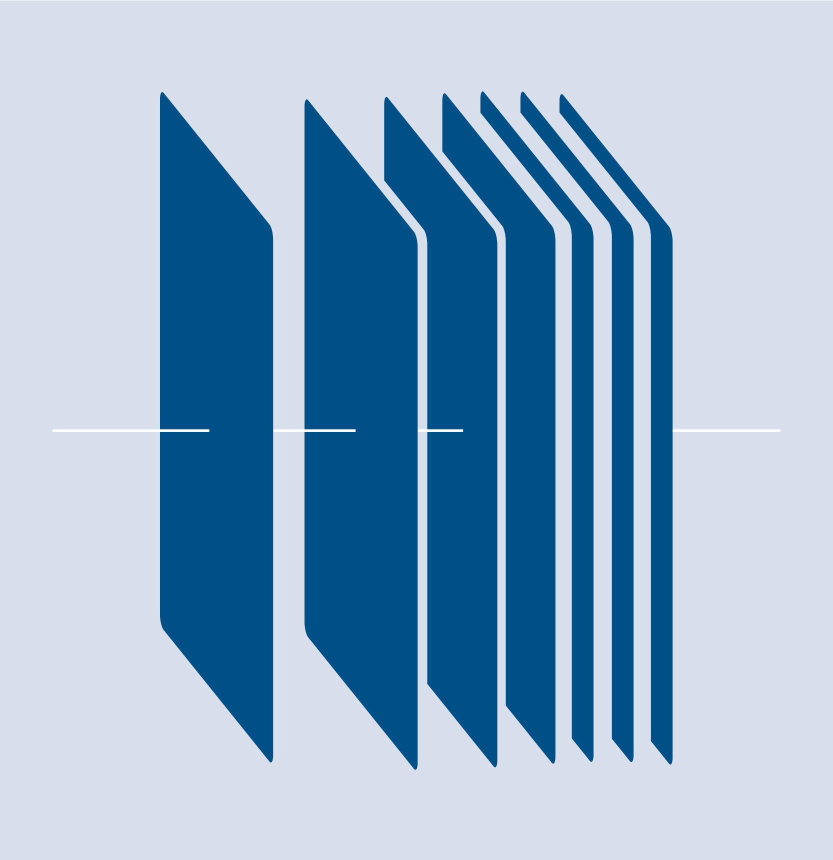
Customer screening takes longer, since screening the account database involves looking at a broad range of data sources, from sanctions and PEP/RCA lists through to adverse media. The aim is to identify accounts that need freezing/blocking, require more detailed due diligence, or could present problems in the future.

Organisations need to screen each customer during the onboarding process, as well as screening their entire databases regularly to identify the level of risk posed by each customer. Large banks typically screen every night against new-to-bank and new-to-list names, as well as existing clients. Smaller banks may screen on a weekly or monthly basis, depending on their risk appetite and size of their customer database.

If a customer is identified by the screening solution as being on a PEP or RCA list, the first question will be whether the institution also considers them to be a PEP or RCA in line with their internal policy. If so, the bank might decide to apply a higher level of due diligence to that individual. This is not a one-off exercise, and forms part of a bank's ongoing due diligence efforts. A marker may be applied to the account so that if certain thresholds are breached, an instant review of the account will be triggered. The bank will also carry out annual reviews of high-risk accounts.

Demonstrating effectiveness

Finding and collating the required information can be a manual process, often resulting in inaccurate reporting and inefficient processes. So why not change to an automated process with a centralised audit trail?



Carrying out transaction and customer screening is essential, but it's not the whole story. To keep up with regulatory requirements, banks need to be able to assess, monitor and disclose risk – and prove they are doing so effectively. And they need to be confident they can uncover potential risk without slowing business operations.

Small banks need to demonstrate transparency and compliance to their correspondents. The right screening tools, backed up by clearly auditable processes and controls, can go a long way toward providing such clarity and reducing compliance costs for their correspondents – which helps reduce the chance of de-risking.

How SWIFT can help

Transaction screening

SWIFT Sanctions Screening combines a best-in-class filter with automatically updated sanctions lists to deliver a highly effective "plug-and-play" solution for real-time screening of financial transactions.

As a hosted solution, SWIFT Sanctions Screening is easy to integrate into your compliance processes. It automatically routes messages to a centrally hosted filter, where they are checked against the latest sanctions lists, instantly alerting you to any matches.

Customer Screening

SWIFT Name Screening screens databases and single names against sanctions, PEP, RCA, sanctions ownership and private lists.

This hosted service can easily be tailored to local regulatory requirements and institutional risk policies. SWIFT manages list updates as they occur, while built-in reporting provides a full audit trail; a cost-effective way to implement a secure, industry-standard screening programme.

Test your screening controls

SWIFT Sanctions Testing provides independent quality assurance for your sanctions filters.

The hosted service leverages the SWIFT compliance expertise to test, fine-tune and optimise your transaction, customer and PEP filters. The fully automated solution helps you maintain full control over your sanctions compliance processes while improving their performance and managing costs.

Detect and prevent fraudulent transactions

SWIFT Payment Controls monitors transactions and prevents out of policy behaviours in real-time.

This service enables you to take the appropriate measures to mitigate business disruption and financial losses in the unlikely event that fraudsters compromise the institution's payments operations environment.

For more information, visit **www.swift.com/compliance** or contact your SWIFT account manager.

57386 - July 2018