The SWIFT Traffic Profile
Unique, value-added report helps correspondent banks pinpoint potential risks from sanctioned or high-risk jurisdictions

Regulators and compliance experts agree that transparency is the foundation of successful compliance programmes. The bar has been raised, and Know Your Customer (KYC) compliance – while of critical importance – is no longer enough. Financial institutions are expected to know their customers’ customers and counterparties as well.

Obtaining next level information about who your counterparties are doing business with isn’t easy however. Until now, financial institutions have had to rely on the declared behaviour of their banking partners. Authenticating such information requires extensive investigation and follow-up discussions. It leaves institutions in the dark about possible risks from counterparties, without a means to visualise and evaluate that risk.

As the secure, global network over which the majority of correspondent banking transactions take place, SWIFT is uniquely able to offer a global solution to the Know Your Customer’s Customer (KYCC) challenge.

The SWIFT Traffic Profile provides a clear, at-a-glance view of an institution’s SWIFT message traffic involving jurisdictions that are subject to close monitoring by FATF, or are sanctioned by the European Union or OFAC. This set of reports contains easy-to-understand, factual data which institutions can use in their KYC risk assessments. They can also share their reports securely with their counterparties, using The KYC Registry.

The SWIFT Traffic Profile is available through The KYC Registry as an additional service. It is computed at the level of the individual legal entity in The KYC Registry and always relates to a single BIC. Banks must sign up to use the Registry in order for SWIFT to create their Profile.

Unique value-added information

Your SWIFT Traffic Profile reports are based on aggregated FIN message traffic for Payments and Trade Finance. Each of these markets is covered separately in a set of three reports that provide increasing levels of detail.

Level 1 (Aggregate Exposure) reports show whether your institution has been directly or indirectly exposed to transactions involving high-risk or sanctioned countries, and the aggregate level of such exposure.

Level 2 (Country Exposure) reports indicate the share of each individual jurisdiction within your institution’s total exposure. You can share your institution’s Level 1 and Level 2 reports with selected counterparties at your discretion, using The KYC Registry.

Level 3 (Counterparty Exposure) reports identify which counterparties are responsible for the risk exposure measured in Level 1 and 2 reports. Level 3 reports cannot be shared through The KYC Registry.

Benefits
- Independent and fact-based
- Unique insights into counterparty data
- Manage CDD enquiries more efficiently and effectively
- Full access control over shared data
- Substantiates declared behaviour
- Continuous risk monitoring
SWIFT Traffic Profile - Level 1
Is the bank exposed to high-risk or sanctioned jurisdictions?

<table>
<thead>
<tr>
<th>Counterparty</th>
<th>Counterparty (country)</th>
<th>RECEIVED from counterparty</th>
<th>SENT to counterparty</th>
<th>Country of exposure is ORDINANCE</th>
<th>Country of exposure is BENEFICIARY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bank A</td>
<td>United States</td>
<td>X</td>
<td>x</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank D</td>
<td>Germany</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bank E</td>
<td>Belgium</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The SWIFT Traffic Profile identifies risk exposure from countries that are considered to be High Risk by FATF or are under EU or OFAC sanctions.

SWIFT Traffic Profile - Level 2
Which jurisdictions does the exposure come from?

The SWIFT Traffic Profile indicates exposure to transactions involving high-risk or sanctioned jurisdictions. Level 1 identifies the existence of exposure, Level 2 identifies the countries responsible for the exposure, and Level 3 indicates which institutions are the source of the exposure.

Up-to-date information
SWIFT Traffic Profile reports are refreshed on a quarterly basis. SWIFT continuously monitors the lists of sanctioned and high-risk jurisdictions and performs additional updates when the lists change, so your reports are always based on up-to-date list and traffic information.

Remain firmly in control
As the “publishing” institution, you always remain in control of which institutions can view your SWIFT Traffic Profile reports in The KYC Registry. You can decide which level of details is shared, and access can be granted or revoked at any time.

A strict publication process lets you verify, sign off and comment on your reports before sharing them with your selected counterparties.

Benefits for publishers and consumers
Sharing your SWIFT Traffic Profile with selected counterparties helps you develop and strengthen (new) business relationships by demonstrating the soundness of your network and compliance practices. It helps you increase efficiency and reduce response time for Customer Due Diligence (CDD) requests, as you no longer need to retrieve, analyse and compile your own data to substantiate your institution’s declared behaviour.

As a consumer of your counterpart’s SWIFT Traffic Profile, you benefit from truly unique insights that allow you to make better-informed business decisions in line with your institution’s risk appetite. Ongoing due diligence effort is reduced, and you have tangible evidence as to whether your counterpart’s behaviour is in line with your counterparty agreement.

The SWIFT Traffic Profile also helps to foster continuous risk monitoring by identifying changes in counterparty behaviour.

Download sample SWIFT Traffic Profile reports and watch related videos at www.swift.com/swiftprofile.

For more information about The KYC Registry, contact your SWIFT account manager or visit www.betterKYC.com