



**Financial Crime
Compliance Services**

Setting the standard in financial crime compliance

Easing your compliance burden

Multiple factors make compliance with financial crime legislation one of the most difficult challenges facing institutions operating in today's financial markets.

In response to ever more sophisticated financial crime threats, regulators around the world are raising the bar on banks' sanctions, counter terrorist financing (CFT), anti-money laundering (AML), know your customer (KYC) and cyber security requirements. And fines for lapses are at record levels. New technological, financial and operational challenges are emerging, and evolving cyber threats highlight the need for robust fraud prevention programmes and practices.

Proven solutions to shared challenges

SWIFT connects financial institutions across the globe, enabling them to transact business quickly, securely and cost-effectively. To protect our community, we offer a broad suite of financial crime compliance products to help you tackle financial crime head-on.

With customers in more than 200 countries using our compliance services portfolio, we help you set the standard in terms of effective regulatory compliance, greater transparency and more efficient operations. And, as cyber threats evolve, we are adding fraud solutions as part of our Customer Security Programme.

But we aren't stopping here. Our compliance vision and roadmap is driven by customer requirements and informed by close engagement with senior compliance professionals from across our global community, so it will evolve in line with your needs. By leveraging industry-defined standards, a common infrastructure and shared costs, we deliver innovative compliance solutions to address industry-wide challenges – in close collaboration with you, our customers.

Over **65%** of customers say their company's AML department handles fraud detection and prevention.

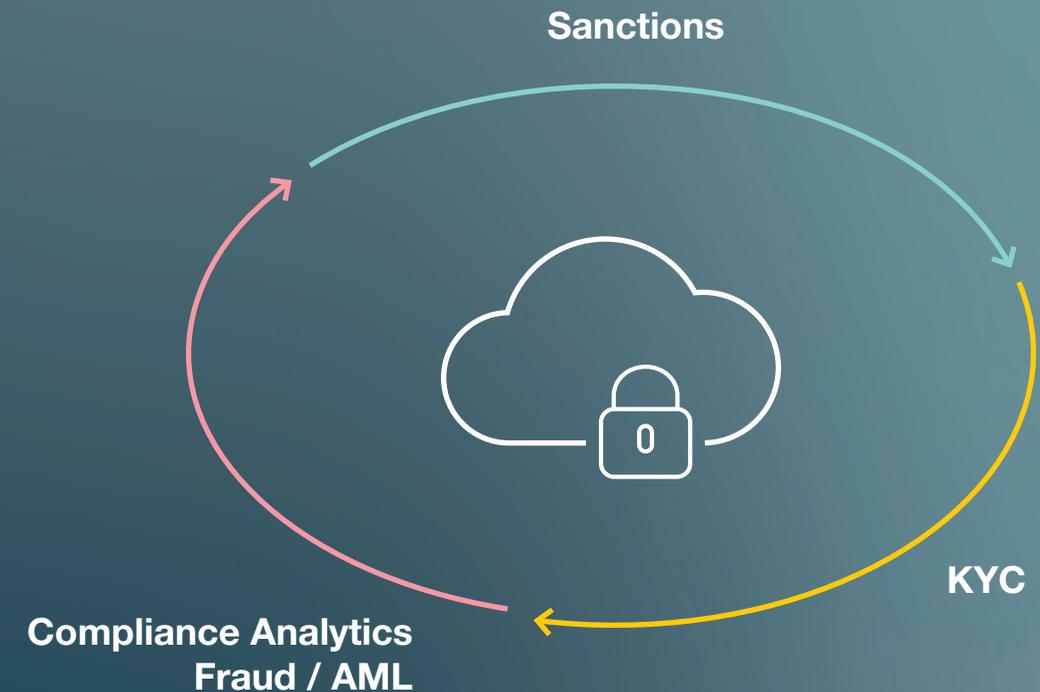
Dow Jones & SWIFT 2017 Global Anti-Money Laundering Survey

Nearly **60%** of customers say RegTech has helped them to handle AML, KYC and sanctions requirements. And more than half plan to increase RegTech investments in the next 3-5 years.

Dow Jones & SWIFT 2017 Global Anti-Money Laundering Survey

Our utility vision

Secure, hosted SWIFT solutions



✔ Shared case management, data and reporting across various products and services.

✔ Developed with advice from senior compliance experts and user groups.

✔ Evolution over time to address the needs of all SWIFT users.

Sanctions

Optimise sanctions compliance with pinpoint precision

The expansion of international sanctions and governmental efforts to fight terrorism pose a range of evolving challenges for compliance departments.

You need to check a wide variety of available information against rapidly growing lists of sanctioned individuals and organisations, which can be inconsistent and lack standardisation. Automated filtering tools generate false positives and false negatives, meaning follow-up searches must be conducted manually, which is time consuming and risky.

Optimise compliance with SWIFT's help

You can take control of the sanctions compliance process with maximum accuracy, efficiency and cost-effectiveness using our modular set of sanctions compliance services. These include transaction and name screening against standardised sanctions lists, with integrated reporting and case management.

Our unique shared services approach can help you standardise and optimise your screening processes in line with market practice.

Sanctions Screening

Streamline your transaction screening

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, Sanctions Screening is easy to integrate into your compliance processes. It checks incoming and outgoing messages against more than 30 of the most commonly used public sanctions lists, as well as researched sanctions ownership lists. Sanctions Screening can screen all structured message formats, including messages sent over networks other than SWIFT.

SWIFT manages list updates, including quality checks, so you know the lists you are using are always up-to-date. You can also add and manage your own private and white lists to boost your own efficiency.

SWIFT's Sanctions Screening's advanced fuzzy matching capabilities detect possible matches using logical tests to highlight intentional and unintentional errors, such as anagrams, letter inversions, missing letters, misspellings, abbreviations and phonetic similarities.

For added reassurance, SWIFT commissions regular independent reviews of the effectiveness of the Sanctions Screening tool. These reports help you demonstrate internally and to your overseers that you have the appropriate screening processes and controls in place.



The implementation of Sanctions Screening was extremely simple, enabling us to finish the project, including the training period and approval phases, in record time.

Eládio Ibiapina Bezerra
Superintendent of Information Technology,
CCB Brazil



With Sanctions Screening we now have a level of comfort and confidence that allows us to meet our sanctions compliance requirements.

Andrea Saracini
Head of Business Applications of Payment
Systems, Iccrea Banca

Benefits

- Easy to implement
- Reduces compliance costs
- Increases efficiency
- Third-party quality assurance
- Peace of mind

Sanctions Testing

Test and optimise filter and list performance

In addition to having transaction, name and PEP screening systems in place, regulators expect you to prove that these systems are effective in preventing business with sanctioned entities. You also need to demonstrate an understanding of how your filters work and why you have adjusted the filter settings. Sanctions Testing helps you provide such proof internally and to your overseers. It assesses your list coverage and content, evaluates true hit and fuzzy matching performance, and uses iterative testing and tuning to help you increase filter efficiency. The tool is unparalleled in its ability to exhaustively test every sanctions and PEP list in scope, using proven standards and methodology developed by SWIFT with its community.

As a secure SWIFT-hosted service, Sanctions Testing is easy to implement and requires minimal maintenance. You can automate testing at predetermined intervals or when triggered by specific events, and can align testing with your compliance and risk policies. The Peer Assessment feature, an optional add-on, lets you evaluate the performance of your filter against data from other participating users with similar business and risk profiles.

To further enhance the benefits, SWIFT organises regular user group meetings for Sanctions Testing customers to share best practices within confidential settings.

List and filter testing can also be delivered on a consultancy basis.



Sberbank has acquired a number of subsidiaries in Central Europe and the Middle East in recent years. These banks have different sanctions filtering technologies, and are subject to differing local regulations. SWIFT's Sanctions Testing service is helping us evaluate filter performance and implement changes where necessary in order to optimise screening effectiveness and efficiency and mitigate cost and risk related to our sanctions compliance programme.

Larissa Zalomikhina
Head of Compliance, Sberbank

Benefits

- Ensures filter effectiveness and efficiency
- Model validation and fuzzy effectiveness measurement
- Delivers assurance, insight and superior understanding
- Ability to manage your risk appetite and alignment to policies
- Automates, simplifies and streamlines filter test cycles



SWIFT tested our filters and delivered a detailed assessment, which provided transparency around our filter settings and their alignment with our risk appetite. We've reduced customer screening filter alerts by 40 percent, and payment screening filter alerts by 60 percent with the help of SWIFT and our filter supplier.

Richard Moore
Managing Director, Group Head of Financial Crime & Security Services, DBS

Name Screening

Fast, accurate screening of customer and supplier names

Name Screening screens databases and single names against sanctions, PEP and private lists quickly and accurately. The tool combines a powerful filter with comprehensive data sources to ensure accurate results, with built-in rules to reduce false positive alerts.

As a secure SWIFT-hosted solution, Name Screening provides automatic sanctions list updates, alerts and case management. The batch screening function enables you to screen entire databases at once, and automate the process on an ongoing basis. And screening individual customers is as simple as an internet search.

Name Screening is easy to integrate into your compliance processes. SWIFT ensures data security and confidentiality in line with its stringent standards and EU privacy laws.

For your assurance and peace of mind, we commission regular independent reviews of the Name Screening service's effectiveness, allowing you to demonstrate that you have the appropriate controls in place.

Nearly 90% of compliance officers expect internal lists to be updated within 24 hours of changes to official lists.

Risk-based decisions and guidance from local AML regulations continue to be the most widely used methods in choosing which lists to use in client screening. These two methods both increased in 2017 while the impact of system capabilities decreased.

Dow Jones & SWIFT 2017 Global Anti-Money Laundering Survey

Benefits

- Fully hosted, with zero maintenance
- Individual or batch delta screening
- Automatic list updates handled by SWIFT
- Get assurance through full audit/quality assurance reporting

Sanctions List Distribution

Sanctions List Distribution packages the most commonly used public watch lists for download in standardised formats.

Standardisation and data enrichment increases filter effectiveness and efficiency, especially for customer database screening.

SWIFT updates the lists when changes are published by regulators, giving you continuous access to the latest watch list data.

Sanctions List Distribution eliminates the need for you to source and reformat lists yourself, helping you to remain compliant when lists change.

Customer due diligence



BWO KYC

? Do I have enough information to make an informed decision to do business with this entity?

Customer screening



NSS

? Is this prospective customer on a sanctions list? Are they a PEP?

Risk profile identification



NSS KYC

? How do I best manage risk associated with this customer?

Start business



RMA RMA+

? How can I efficiently manage the business I do with this customer?

Screening transactions and databases



NSS PC PDQ SLD SSS

? Are the transaction messages I exchange with this customer compliant and aligned with risk policies?

Ongoing due diligence



KAM KYC SAA STP

? How can I ensure that I understand my customer's business and any changes that might affect my risk exposure?



Behavioural monitoring

CA CM DVR STS

? Does my business adhere to our compliance and risk policies and can we demonstrate this?

Meeting your needs every step of the way

Sanctions

NSS

Name Screening

lets you screen prospective customers against sanctions, PEP and private lists. Batch screening helps you keep your customer and vendor databases compliant with sanctions and risk requirements

SLD

Sanctions List Distribution

packages watch lists in standardised XML format

SSS

Sanctions Screening

screens SWIFT and non-SWIFT messages against public and private lists

STS

Sanctions Testing

automates testing of transaction, customer and PEP filters and lists for better screening performance and assurance snapshot of SWIFT activity

KYC

BWO

Banker's World Online

helps you prospect for new relationships

KAM

KYC Adverse Media

provides negative news and regulatory notifications for your onboarding and ongoing CDD processes

KYC

The KYC Registry

makes conducting initial KYC more efficient, so you can start doing business faster. It also supports ongoing due diligence by alerting you to important changes at counterparty institutions

SAA

The KYC Registry Security Attestation Application

supports cyber-risk management and business decision making

STP

SWIFT Traffic Profile

reports show users' exposure to sanctioned or high-risk jurisdictions

Compliance Analytics / Fraud / AML

CA

Compliance Analytics

pinpoints compliance risk across your (global) operations

CM

Correspondent Monitoring

delivers top-down AML monitoring and alerting

DVR

Daily Validation Reports

enhance existing fraud controls with an independent daily activity

PC

Payment Controls

blocks fraudulent or suspicious transactions (Coming in 2018)

PDQ

Payments Data Quality

helps banks comply with FATF Recommendation 16, and enhances transparency and straight-through processing

RMA RMA+

RMA and RMA+

helps you manage business relationships

Know Your Customer (KYC)

Establish and strengthen correspondent banking relationships

In recent years, stricter KYC obligations have had major cost and efficiency implications for correspondent banking.

KYC data collection diverts time from business activities and relationship management, and requires the verification of massive amounts of non-standard data and documentation. The difficulty and cost of sourcing accurate KYC information has led some banks to 'de-risk', or terminate correspondent relationships, potentially hampering economic growth.

The KYC Registry advantage

SWIFT is helping banks of all sizes and locations address this challenge. SWIFT's KYC solutions provide access to the most complete and accurate KYC datasets on a secure global platform. Large banks spend less time collecting data, and more time evaluating the risks associated with existing relationships and new clients. Contributing data to The KYC Registry enables smaller banks to demonstrate transparency and compliance to their correspondents, strengthening business relationships, while lowering the associated costs.

The KYC Registry Security Attestation Application

SWIFT introduced the Customer Security Programme (CSP) to reinforce the security of the global financial community. The Customer Security Controls Framework and attestation process helps customers secure their local SWIFT environments, and enhances cyber-risk management across the community.

The KYC Registry Security Attestation Application is the tool for users to submit their self-attestation data to confirm their organisation's level of compliance with SWIFT's customer security controls. Users can share their self-attestation data with their counterparties and request counterparty data in order to apply risk-based decision-making to their business relationships.

As a first step, users submit their institution's self-attestation data to the KYC Registry Security Attestation Application. Thereafter, they can search the application for attestations published by other institutions and request access to this data.

The KYC Registry

Monitor, manage and grow your correspondent banking network

The KYC Registry is a global repository of up-to-date due diligence documents and data for correspondent banks and funds players. It provides a single, central source of KYC information, which SWIFT validates and checks for completeness and accuracy.

The Registry enables you to monitor, manage and grow your correspondent network quickly and cost-effectively. You can contribute your institution's data so that others can access it, replacing the need to respond individually to each incoming KYC request. Each member institution retains responsibility for its KYC information, and control over who has access to it.

Available to Registry subscribers, KYC Adverse Media informs you when counterparties are the subject of negative press coverage and regulatory notifications. It addresses regulatory expectations to consult news sources as part of ongoing customer due diligence (CDD) processes.

SWIFT Traffic Profile reports detail your exposure to message traffic from sanctioned and high-risk jurisdictions, and the source of this exposure. You can exchange Profile reports with your counterparties using The KYC Registry.

Benefits

- Access to high-quality KYC data, verified by SWIFT
- Stronger, more transparent relationships
- Simpler onboarding process
- Better operational efficiency
- Value for money



The KYC Registry's broad coverage and focus on correspondent banking is important – and the standard baseline of information in the Registry fits very well with our internal policy.

Michael Kohn
Global Head of Corporates & Investment Banking KYC Programme, UniCredit



SWIFT's KYC Registry includes a number of unique elements which make it particularly suited to Lloyds Bank's compliance needs. As a member-owned, not-for-profit cooperative, SWIFT occupies a position of trust in the market. Trust is crucial where data-sharing is concerned.

Mark Brotherton
Director, Fraud & Financial Crime, Lloyds Bank Commercial Banking

More tools to support compliant correspondent banking relationships

The KYC Registry's robust dataset is complemented by SWIFTRef Banker's World Online – your source for payments reference data, and an invaluable tool when prospecting for new relationships.

With the heightened focus on cyber security, SWIFT's Relationship Management Application (RMA) and RMA+ help you protect your institution against fraudulent or unwanted message traffic. Use them to manage which institutions you do business with, and what types of messages you exchange.

Compliance Analytics

Unique data, world-class analytics

As regulatory pressure grows in response to ever more sophisticated money laundering techniques, existing AML tools no longer address the needs of correspondent banks. Advanced data analysis is also vital in the fight against evolving cyber threats. At the same time, data volumes are increasing exponentially; these datasets lack standardisation, are often spread across multiple IT systems and subsidiaries, and are delivered in multiple formats.

As the international banking community unites in its efforts against money laundering, terrorist financing and cyber fraud, reactive approaches to financial crime fall short and can lead to financial loss and reputational damage.

Leverage your SWIFT data to enhance compliance

SWIFT's Compliance Analytics solutions help you to comply with global regulatory standards by providing a comprehensive dataset of your SWIFT message traffic. A comprehensive portfolio of services helps you identify, monitor, analyse and address compliance and fraud risk, keeping your business on the right track.

Compliance Analytics

Analyse and monitor your organisation's SWIFT transactions

Compliance Analytics leverages your institution's SWIFT message data to provide an unparalleled level of insight into your banking flows, enabling you to monitor and address financial crime risk with absolute accuracy.

By providing a truly global view of message traffic, Compliance Analytics helps you identify possible anomalies in behaviour, unusual patterns or trends, hidden relationships and consistently high levels of activity with high-risk countries and entities. It supports compliance across a range of domains, including KYC, AML and Sanctions.

The secure, user-friendly analytics platform uses data visualisation to aid analysis and generates alerts when it detects activity spikes, outliers or policy breaches.

Compliance Analytics lets you compare your traffic with global aggregated SWIFT traffic, highlighting, for example, your share of payments traffic in particularly high-risk countries. Its standardised data set saves you time and money and avoids the need for costly IT intervention or systems integration.



Organisations are swimming in data that's not aggregated and in one place. Compliance Analytics provides a single source of rich, standardised data, and I would recommend it on that basis alone.

Naylor Dray
Director, Business Assurance, FI AML Monitoring, ANZ



With Compliance Analytics, our financial intelligence unit can quickly find an entity involved in an unusual transaction using its name and the name of the beneficiary. We can also delve deeper into the SWIFT message data and find out if this entity has any hidden relationships or additional wire transfers with other entities.

Daniel Del Rosal
Managing Director of Compliance, CIBanco

Benefits

- Mitigates risk
- Comprehensive view of message traffic
- Enhances efficiency
- Reduces costs
- Provides peer group comparison

Compliance Analytics Solutions

Payments Data Quality

Payments Data Quality helps you evaluate the quality of originator and beneficiary information in your payment messages, using advanced data analytics. You can identify which branches and counterparties (regularly) send messages with poor quality data, and take appropriate action using fact-based reporting. And, as a secure, web-based service, you can sign up and start using the tool right away.

Developed by SWIFT in collaboration with its community, Payments Data Quality supports strong compliance and operational performance on three levels.

First, it aids compliance with originator and beneficiary data requirements related to Financial Action Task Force (FATF) Recommendation 16, including the 4th EU AML Directive, as well as the US Travel Rule. In addition, by helping banks to improve data quality, the service also provides for greater transparency and stronger sanctions and AML controls.

Finally, Payments Data Quality enhances operational efficiency and straight-through processing by identifying areas in which poorly formatted messages are being blocked or delayed, so you can take appropriate action.

Benefits

- Supports compliance with FATF 16 and related regulation
- Helps improve message data quality
- Enhances operational efficiency
- Mitigates risk
- Cost efficient



Payments Data Quality has enabled us to set up better operational flows and improve straight-through processing rates. It gives us the extra assurance that we are in control, and are able to prove it. That's really a great benefit.

Joyce Verschaeren
Head of Operations Control and Services Development, Rabobank

Correspondent Monitoring

Our Correspondent Monitoring tool delivers top-down AML monitoring and alerting, tailored to correspondent banking requirements. It captures information about your transactions over the SWIFT network, so you can analyse end-to-end bank flows.

Correspondent Monitoring helps you understand and analyse the parties involved in the payment chain, nested relationships, the locations involved, and whether transactions fall outside of normal or expected activity. Risk-scoring and modelling help you identify high-risk areas, and you can set parameters for automatic notifications when further investigation is needed.

The tool supports in-depth KYC reviews of correspondent activities and facilitates a risk-based approach to correspondent banking AML compliance by highlighting higher-risk payment flows for additional controls in line with your institutional policies.

Fraud Control Solutions

Daily Validation Reports

With the recent surge in cyber threats, Daily Validation Reports are a vital part of SWIFT's Customer Security Programme to help protect the global financial community.

Activity reporting shows aggregated value and volume data for inbound and outbound messages, along with comparisons against your daily volume and value averages over the previous 24 months, allowing any significant changes in activity to be quickly identified.

Risk reporting highlights large or unusual single transactions and aggregated transactions by counterparty – and also flags new combinations of direct and indirect counterparties appearing in transactions during that day.

In recent wire fraud attacks, fraudulent messaging activity has been concealed on targeted banks' local systems by deleting logs and manipulating data records. Daily Validation Reports help to mitigate the risk of lost records by providing daily activity and risk reporting of your previous day's SWIFT transactions. Reports are delivered via a completely separate, secure online channel, direct to your compliance or operations teams for monitoring.

Benefits

- Independent data source
- Rapid risk identification
- Faster incident response
- Secure delivery via secondary channel
- Easy to use and customise

Over 65% of respondents work in companies in which the AML department handles fraud detection and prevention, an increase from 2016. Risk data remains the most relevant information for managing fraud, followed by crime typologies and news.

Dow Jones & SWIFT 2017 Global Anti-Money Laundering Survey

Payment Controls

As part of its Customer Security Programme (CSP), SWIFT has created a new Payment Controls service to provide in-network screening of payment messages before they are sent.

Developed in cooperation with the SWIFT community, Payment Controls will enable users to identify, investigate, block and prevent fraudulent or out-of-policy payments in real time. It protects subscribing institutions from potentially fraudulent transactions based on their risk policy settings.

The service 'learns' each customer's payment patterns over time and highlights high-risk payment instructions involving new counterparties, currencies, message types or combinations of these. You can choose your own screening parameters to allow timely detection and help prevent fraudulent transfer requests.

Payment Controls augments existing fraud prevention controls and is designed for seamless integration with business, compliance and operational processes. It complements the reporting provided by Daily Validation Reports and will initially address the needs of smaller institutions.

Payment Controls will be commercially available in 2018.



Discover the value of working with SWIFT

For more information, visit us at www.swift.com/complianceservices or contact us at compliance.services@swift.com.

About SWIFT

SWIFT is a global member-owned cooperative and the world's leading provider of secure financial messaging services.

We provide our community with a platform for messaging, standards for communicating and we offer products and services to facilitate access and integration; identification, analysis and financial crime compliance.

Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way.

As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies.

Headquartered in Belgium, SWIFT's international governance and oversight reinforces the neutral, global character of its cooperative structure. SWIFT's global office network ensures an active presence in all the major financial centres.

For more information, visit www.swift.com or follow us on Twitter: [@swiftcommunity](https://twitter.com/@swiftcommunity) and LinkedIn: SWIFT