Information Paper

RMA and RMA Plus: managing your correspondent connections

SWIFT's financial crime compliance products help financial institutions understand, manage and mitigate operational, compliance and fraud risks in line with industry recommendations.

Contents

SWIFT’s financial crime compliance products help financial institutions understand, manage and mitigate operational, compliance and fraud risks in line with industry recommendations.

Against a backdrop of stricter regulations and enforcement actions, it is more important than ever for financial institutions to manage their correspondent connections effectively. SWIFT’s Relationship Management Application (RMA) plays an important part in supporting communication between different financial institutions.

What is RMA?

> The use of RMA or RMA Plus is mandatory for user-to-user messages that require end-to-end signature, which covers most types of SWIFT FIN messages.

The RMA is a SWIFT-mandated authorisation that enables financial institutions to define which counterparties can send them FIN messages. RMA is the Relationship Management Application, though in common use when discussing an RMA, what is described is the key exchange and authorisation process between two institutions. Any unwanted traffic is blocked at the sender level, reducing the operational risks associated with handling unwanted messages. In order to facilitate transactions, RMAs can also be established with non-customers – in other words, counterparty financial institutions of the bank for which the bank does not hold an account.

RMA Plus, the more granular version of RMA, goes one step further by letting institutions specify which message type(s) they want to send to, and receive from each of their counterparties. For example, an institution might only wish to receive letters of credit from a particular correspondent. By giving greater control over individual relationships, RMA Plus can facilitate new business opportunities which might otherwise be avoided due to risk and regulatory concerns.

The use of RMA or RMA Plus is mandatory for user-to-user messages that require end-to-end signature, which covers most types of SWIFT FIN messages. Institutions need to grant RMA or RMA Plus authorisation to their counterparties in order to receive messages from those counterparties. RMA functionality is built into the Alliance Access and Alliance Entry SWIFT interfaces, and Alliance RMA is also available as a standalone product.

RMA and due diligence

When RMA was introduced in 2009 as a replacement for the Bilateral Key Exchange (BKE), the spirit of the product was for banks to open the door to as many counterparties and correspondents as possible. Today, however, the more stringent regulatory climate means that many institutions are now rationalising their correspondent banking relationships in order to remove higher risk correspondents and to help to reduce the risk of fraudulent transactions. Banks today would rather keep the door open only to parties they trust and want to do business with – and shut other doors in order to avoid potentially problematic transactions.

As such RMA is increasingly seen as a compliance control. Indeed, some regulators require banks to do full due diligence on their correspondents whenever an RMA is present, regardless of whether a business relationship is actually in place.

A guidance paper published by the Wolfsberg Group in May, *"Wolfsberg Guidance on SWIFT Relationship Management Application (RMA) Due Diligence"*, highlights the link between using RMA and conducting due diligence. The paper notes that financial institutions "should incorporate RMA due diligence standards into their Financial Crime/ AML/KYC programmes", citing a number of principles which should be considered both for customer and non-customer RMA relationships.

> **"Financial institutions should incorporate RMA due diligence standards into their Financial Crime/ AML/ KYC programmes**
>
> **Wolfsberg Guidance on SWIFT Relationship Management Application (RMA) Due Diligence**

Managing RMAs more effectively

RMAs also have implications from a risk management point of view. By using RMAs, financial institutions can reduce their exposure to the operational risks associated with handling unwanted messages. However, the definition of unwanted traffic can change over time.

Sometimes financial institutions will decide that they no longer want to receive messages from a specific counterparty. In other cases, institutions may simply find that they have not received messages from a particular correspondent for a long time. Either way, risk exposures can arise if banks do not keep their RMA authorisations up to date

At many institutions, the list of RMA authorisations is not always updated when business relationships change or are terminated. Institutions may therefore have a large number of inactive RMAs in place – and may not even be aware of them. Tracking these RMA and RMA Plus relationships can be challenging, particularly for large organisations with multiple payments systems, dozens of branches, and hundreds or even thousands of correspondent relationships.

This can mean additional cost and effort for customer due diligence (CDD) activities on open RMAs, as well as opening the door for unwanted message traffic. Legacy RMAs can also create the opportunity for payments to be sent to destinations which may no longer be wanted or authorised, resulting in fraud risk.

By rationalising dormant or inactive RMAs, institutions can minimise the time and cost associated with such activities, as well as reducing risks. RMA authorisations can be revoked by sending an RMA revocation message. SWIFT has also launched a central revocation check which blocks traffic from a ‘revoked’ counterparty within 15 minutes of when the SWIFT network acknowledges a revocation message. In addition, the following services can be used to manage RMA and RMA Plus authorisations:

Maintain a global overview of RMAs

SWIFT’s Compliance Analytics service helps financial institutions track the status of RMAs over time, view the geographical distribution of new RMAs, and drill down to understand RMAs in high-risk countries. The service also enables banks to spot potential risks and provides the tools needed to verify whether risk and compliance policies are being followed throughout their networks.

For example, significant volume changes can be tracked for non-customer RMAs, which might indicate the need for additional due diligence, or a change to RMA Plus status

Rationalise connections with expert consultancy

SWIFT can help financial institutions rationalise their RMA and RMA Plus authorisations, giving more control over counterparty relationships. Our expert consultants can:

- Create a list of correspondents with which an institution has exchanged authenticated messages
- Provide details about traffic with these correspondents (date, volumes, value, nature, direction)
- Identify and flag dormant and inactive RMAs
- Compare the institution’s level of dormant and inactive RMAs with peer institutions
- Review usage and presence of RMA Plus authorisations
- Use RMA queries to notify correspondents of the intention to terminate RMAs, and provide them with an opportunity to justify the need to maintain the relationship
- With approval, delete unwanted RMAs and inform counterparties of the change

The Wolfsberg Group's guidance paper sets out the following concepts and principles for RMA and RMA Plus:

- Due to the potential risks that may be associated with the establishment of an RMA, approval of such requests needs to be appropriately controlled
- RMA requests may be segregated between customer relationships and non-customer RMAs, with distinct due diligence criteria for each
- Where an RMA holder has a customer relationship subject to due diligence, the requirements under that due diligence programme will apply
- Due diligence on the RMA holder should consider the message types used by the RMA holder and the risk associated with the activity conducted
- RMA Plus offers certain capabilities to limit the types of SWIFT messages exchanged and may facilitate the determination of due diligence requirements
- Change in RMA usage from a non-customer to a customer relationship should be identified on a timely basis and any additional due diligence required for the customer relationship collected, as per usual customer due diligence standards.

A global source for KYC information

Finally, RMA and RMA Plus should be considered in the context of SWIFT's wider suite of financial crime compliance tools. For example, having an RMA or RMA Plus authorisation with another financial institution typically creates the need for KYC activities. If that counterparty is a customer, the normal KYC procedures apply.

Supporting KYC activities, SWIFT's KYC Registry provides a global repository of up-to-date due diligence documents and data for correspondent banks and funds players. The Registry leverages the SWIFT community of over 7,500 financial institutions with correspondent banking and funds activities order to deliver a central, standardised set of information, which SWIFT validates and checks for completeness and accuracy. SWIFT also offers a KYC Adverse Media service through the Registry, enabling institutions to search for press articles and regulatory notices about their counterparties.

SWIFT offering	What it does	Benefits
RMA	Enables institutions to define which other institutions can send them SWIFT FIN messages	Helps institutions define who they want to do business with
RMA Plus	Enables institutions to define which SWIFT FIN messages they want to send to and receive from each counterparty	Provides additional granularity and control over correspondent relationships, further mitigating operational and compliance risk
Compliance Analytics	Gives banks a powerful analytics tool to obtain a global overview of their RMA and RMA Plus authorisations, with statuses and trends	Helps banks identify potentially risky correspondent relationships and supports effective, targeted compliance and risk-management activities
RMA / RMA Plus consultancy	Provides global lists of RMA and RMA Plus authorisations, related message traffic information to support decision-making about correspondent relationships, and assistance with updating or terminating such authorisations	Fast, cost-effective approach to 'clean up' RMA and RMA Plus authorisations that may not have kept pace with evolving business relationships and compliance practices
The KYC Registry	Provides a global source of KYC and adverse media information on correspondent banks and funds players	Increased efficiency and reduced effort and cost for KYC and CDD compliance activities

About SWIFT

For more than 40 years, SWIFT has helped the industry address many of its biggest challenges. As a global member-owned cooperative and the world's leading provider of secure financial messaging services, we enable more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories to communicate securely and exchange standardised financial messages in a reliable way.

As their trusted provider, we facilitate global and local financial flows, relentlessly pursue operational excellence, and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. We also bring the financial community together to work collaboratively to shape market practice, enable the creation of global standards and debate issues of mutual interest.

SWIFT users face unprecedented pressure to comply with regulatory obligations, particularly in relation to the detection and prevention of financial crime. In response, we have developed community-based solutions that address effectiveness and efficiency and reduce the effort and cost of compliance activities. Our Compliance Services unit manages a growing portfolio of financial crime compliance services in the areas of Sanctions, KYC and CTF/AML.

Financial crime compliance is also a major theme at Sibos, the world's premier financial services event, organised by SWIFT for the financial industry.

www.swift.com/complianceservices

57214 - July 2016