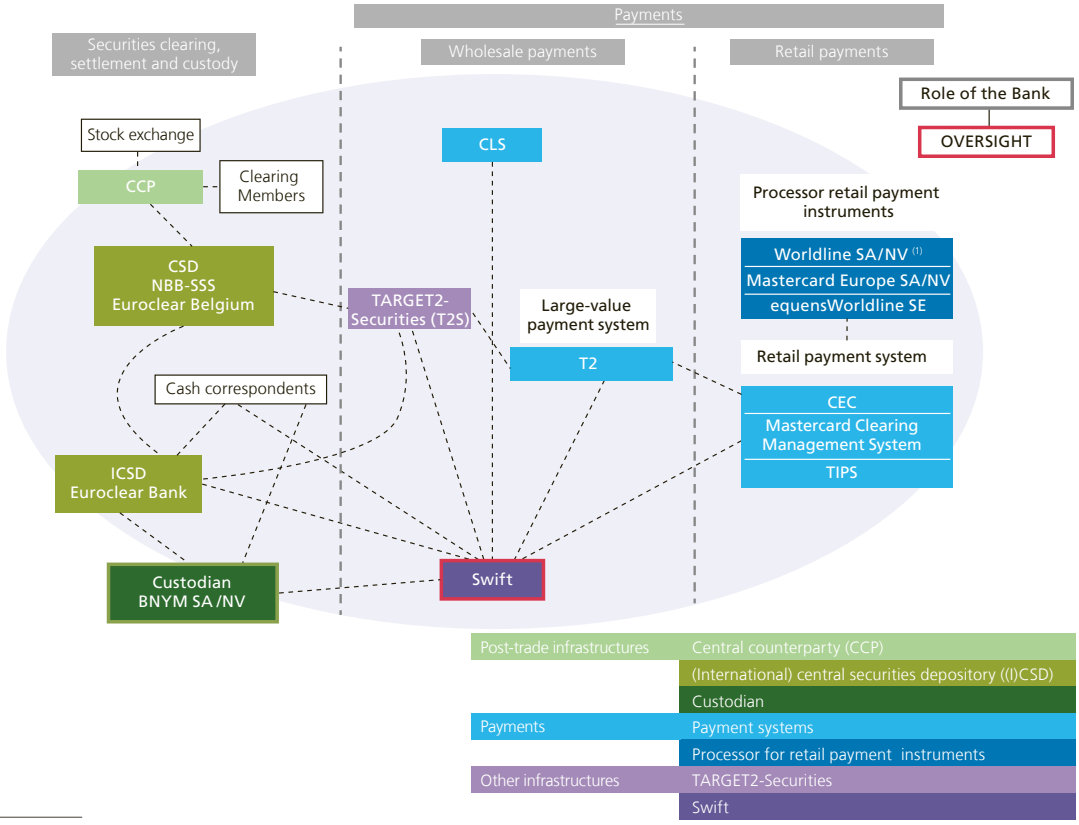
4. Swift

The Society for Worldwide Interbank Financial Telecommunication (Swift) is a limited liability cooperative company that provides messaging services to financial institutions and market infrastructures across the globe. Swift serves different customer types which vary in terms of size and activity: banks, brokers, investment managers, fund administrators, custodians, corporates, and treasury counterparties. Swift is registered in Belgium with its headquarters located in La Hulpe.

Through its financial messaging services, Swift fulfils a crucial role in facilitating correspondent banking and financial market infrastructure activities. Such a fundamental role for the global financial industry creates significant systemic dependency on Swift. Hence, the G10 jurisdictions established the cooperative Swift oversight framework to monitor Swift's activities with the aim of safeguarding financial stability.

Chart 4

Swift as a critical service provider to the financial industry



1 Only the Belgian activities of equensWorldline SE are overseen by the NBB. Worldline Switzerland ltd is also designated as systemic processor for its switching activities for Bancontact according to the Law of 24/03/2017 regarding the oversight of payment processors and has specific obligations in that framework but it is not overseen by the NBB.

4.1 Swift oversight framework

4.1.1 Swift and its users

National member groups are represented by Swift's users and are organised per jurisdiction. These users own and control the company and are involved in the appointment of Swift Board members. Swift's share distribution is based on the message traffic, ensuring that the Board represents the jurisdictions with the largest users, i.e. with the highest message traffic volumes. Since message traffic proportionality is not static, the shares are reallocated every three years to mirror the actual Swift user community. In 2021, such a redistribution took place but did not result in the introduction of any new jurisdictions on the Swift Board. The next share reallocation is scheduled for 2024.

Swift provides messaging services to customers from more than 200 countries, amounting to approximately 11 600 Swift users. The following numbers reflect Swift's global presence: in 2022 11.3 billion messages were sent with a daily average of 44.8 million messages. Despite the global geopolitical tensions and economic uncertainty, Swift achieved a year-over-year growth of FIN traffic of 6.6 % by the end of 2022. The main contributors to this growth were the economic recovery and the securities market volatility, sparked by higher volumes of securities settlement instructions.

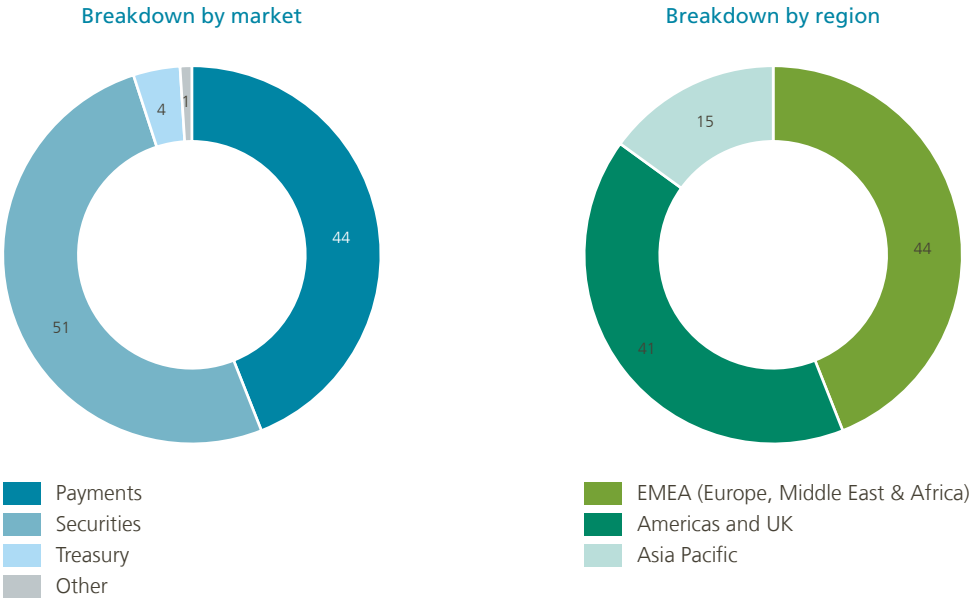
The core messaging service for exchanging financial messages is Swift's FIN application. The figure below depicts Swift's FIN traffic for 2022 distributed per region and market. There was a total of 11 696 live users, of whom 2 360 are Swift's shareholders belonging to different national member groups. In line with figures for previous years, the payments (44.4 %) and securities (50.8 %) markets represented the lion's share of Swift's messaging for 2022. The Europe, Middle East and Africa (EMEA) region claimed the largest part of the total 2022 FIN traffic volume, closely followed by the Americas and UK region.

It is worth noting that, for the ISO 20022 migration for cross-border payments and cash management, use of the FIN messaging service will gradually give way to the FIN Plus service (or InterAct service). A co-existence period, during which users will be expected to switch from the legacy FIN MT to the new ISO 20022 MX format, started in March 2023 and ends in November 2025.

Chart 5

Swift FIN traffic distribution by region and market

(2022)



Source: Swift.

4.1.2 International cooperative arrangement

In 1997, the G10 central banks formalised the Swift oversight arrangement for the purpose of monitoring the adequate and safe functioning of the critical service provider. In addition to the participating G10 jurisdictions, the Bank for International Settlements and the European Central Bank are represented in the international working groups. As Swift is headquartered in Belgium, the NBB is the standing lead overseer and chairs the international oversight meetings.

The G10 central banks are represented in the four working groups: the Technical Group (TG) which conducts technical fieldwork, the Cooperative Oversight Group (OG) which is the decision-making body and sets the oversight strategy, the Executive Group (EG) which serves as the interface for overseers to communicate conclusions and recommendations to Swift's Board and Executive Management, and the Swift Oversight Forum (SOF) which involves a wider group of central banks discussing the oversight activities and relevant changes at Swift.

Given the systemic character of Swift, a wider group of G20 jurisdictions are also directly involved in the oversight. These G20 central banks are represented in the SOF working group. Their membership corresponds to their share in the total Swift traffic volume and the CPMI membership composition. The SOF deals with the Swift oversight conclusions, planning and priorities, Customer Security Programme and discussions on dedicated topics.

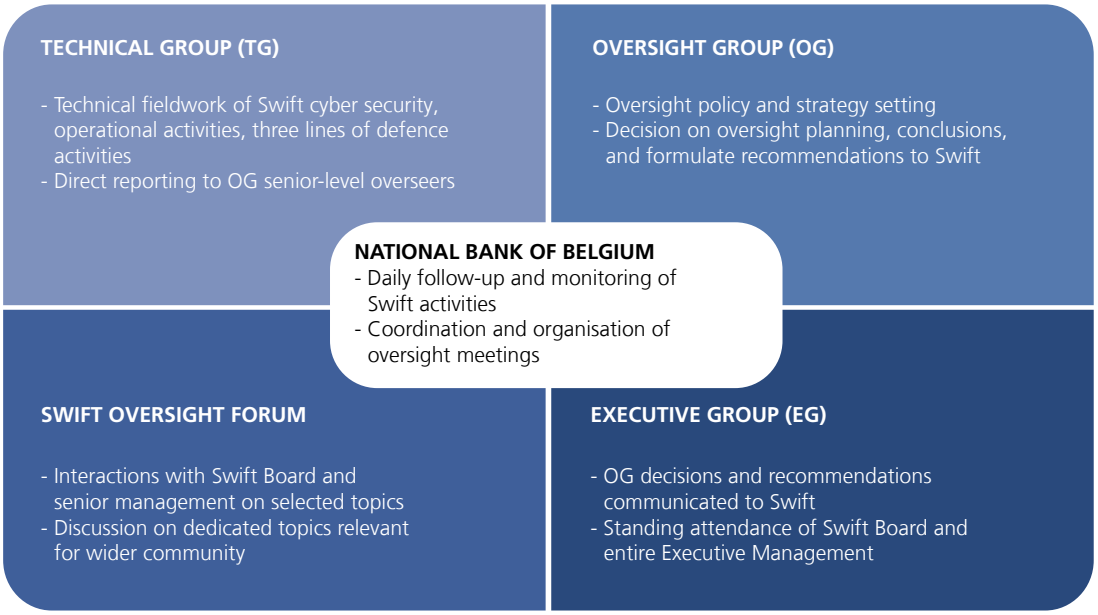
In its capacity as Swift's lead overseer, the NBB has a dedicated team which conducts daily monitoring and follow-up of Swift's activities and projects. As formulated in the Swift Oversight Protocol, the NBB serves as the entry point for channelling information to the other overseers and, as chair, coordinates the different working groups in terms of reporting to the other overseers and preparing discussion items for them.

More detail on the composition and scope of activities for each of the working groups can be found in earlier editions of the Financial Market Infrastructures and Payment Services Report (2017-2021).

The following figure gives an overview of the different working groups involved in the Swift oversight.

Figure

Swift oversight working groups involving G10 and G20 central banks



The oversight on Swift is based on the five high-level expectations (HLEs), i.e. (i) Risk Identification and Management, (ii) Information Security, (iii) Reliability and Resilience, (iv) Technology Planning, and (v) Communication with Users. These five HLEs were set out in Annex F to the CPMI-IOSCO's Principles for FMIs and form the oversight expectations applicable to all critical service providers to FMIs.

The overseers' review activities are all rooted in the five HLEs and drive the oversight planning and priorities. Overseers assess the adequacy of Swift's management of operational and security risks across the three lines of defence (LoDs) by comparing it with these expectations. Swift is thus expected to adhere to the HLEs through appropriate reporting to overseers (i.e. the provisioning of required documentation, interactions with Swift's three lines of defence, and discussions with Executive Management and Board).

More details on the specific description of the five HLEs can be found in earlier editions of the Financial Market Infrastructures and Payment Services Report (2017-2021).

4.2 Selection of major topics reviewed by overseers in 2022

This paragraph covers a non-exhaustive selection of major topics which overseers analysed in 2022. The highlighted topics are a sub-set and not a full representation of the review work conducted in 2022 (e.g. standing topics such as business continuity exercises, effectiveness of three lines of defence, enterprise risk management, and internal audit activities).

4.2.1 Messaging traffic

With 2022 being marked by severe geopolitical unrest and economic uncertainty, as explained in box 10, overseers were keen to analyse the impact of these factors on the growth of Swift's messaging traffic. The fact that Swift could still present high year-to-date traffic growth demonstrates the trust that the global financial community continues to place in the company.

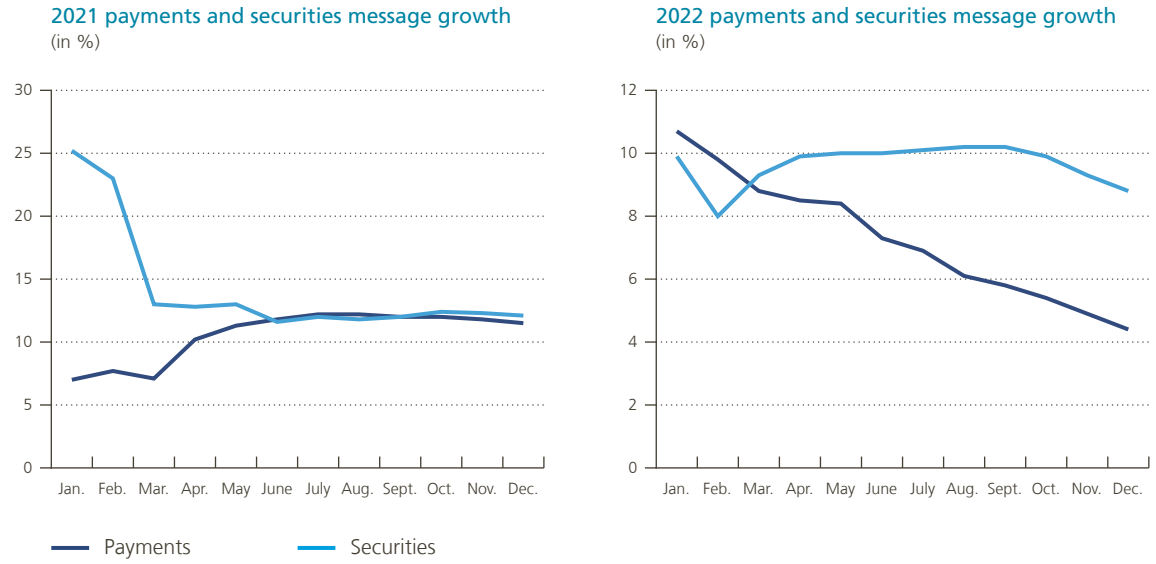
In 2021, there was a marked increase in payments traffic via Swift's network, which could be attributed to the positive outlook following a prolonged period economic uncertainty due to the pandemic. In 2021, Swift's payments traffic grew by 11.5 % compared to 2020 and securities traffic was up by 12.1 % on 2020. Overall, FIN activity recorded 11.4 % growth in 2021.

Given the new challenges posed in 2022 due to the geopolitical tensions, as well as energy crisis and inflationary worries, Swift was still able to provide some solid growth figures. There was strong growth for both payments (4.4 %) and securities traffic (8.8 %), contributing to an overall FIN traffic growth of 6.6 % for 2022.

The following two graphs show the percentage changes in payments and securities traffic growth for 2021 and 2022. Over the course of 2021, growth of payments and securities traffic converged, with both markets recording stable, double-digit growth from mid-2022. The more favourable economic outlook following the COVID-19 pandemic might have been a driving factor for this development. For 2022, Swift maintained positive growth for both payments and securities traffic. Securities traffic posted a growth trend of about 10 % throughout the year, whereas for payments there seemed to be a slight decline in traffic throughout 2022.

Chart 6

Growth of payments and securities message traffic in 2021 and 2022



Source: Swift.

4.2.2 Cyber and physical resilience

Over the course of 2022, Swift regularly reviewed the resilience measures in place, both from a cyber security perspective and from a physical security perspective, ensuring vigilance and readiness in light of any present or future geopolitical tensions. The overseers also stepped up their monitoring of Swift's operations, with weekly updates being provided to overseers up until the end of 2022.

The year 2022 also marked a period of severe turmoil and uncertainty on the energy markets, leading to some countries drafting shutdown plans and reviewing mitigating measures for their critical infrastructures. Viewed as power supply is crucial for the proper functioning of Swift's control centres and datacentres, and thus for the functioning of the global financial markets, this subject also received appropriate attention by overseers. Data integrity and redundancy measures were reviewed, as well as a number of mitigating measures in place, such as uninterruptable power supplies (UPS) and back-up generators and the required fuel supplies.

4.2.3 Customer Security Programme

The Customer Security Programme (CSP) has been a recurring topic on the overseers' agenda ever since the programme was introduced following the 2016 Bangladesh case. Swift has built up an extensive programme enhancing its users' cyber security, their counterparts, and the entire community. Through the CSP, users are required to adhere to certain controls and good practices to appropriately secure their on-premises IT environments connecting to the Swift network. With cyber-attacks continuing in the financial sector, overseers are seeking reasonable assurance on the effectiveness of the CSP and corresponding initiatives, designed to adapt to new threats, improve cyber security capabilities, and adhere to regulatory expectations.

Over the years, Swift has taken multiple initiatives and improved various aspects of the CSP, such as the yearly review of the Customer Security Control Framework (CSCF), improvements to the Know-Your-Customer (KYC)

tool, launch of an Independent Assessment Framework (IAF), introduction of mandated assessments, more effective involvement of supervisors, actionable updates on the Information Sharing and Analysis Centre (ISAC) portal, and organisation of recurring awareness campaigns. Thanks to these actions, Swift has informed overseers that there has been a downward trend in customer cases. In fact, for the first time since the inception of the programme, no fraudulent messages have been sent over the Swift network during both 2021 and 2022. Additionally, not a single customer case was reported during 2022, demonstrating the CSP's effectiveness. On account of its successful track record and promising results, Swift is expected to continue to enhance the programme.

One such expectation concerns the involvement of supervisory authorities in using the CSCF self-attestation data of financial institutions. From the outset, overseers have encouraged Swift's move to engage supervisors more directly in making effective use of the rich self-attestation data of its users, which could provide crucial input for supervisors' risk-based planning and scoping. The identification and onboarding of the relevant supervisory authorities in the Know-Your-Supervisor (KYS) tool have proven to be challenging because some jurisdictions have multiple supervisory authorities relevant for one country. According to Swift's first reporting to overseers on the use of the self-attestation data by the onboarded supervisory authorities for financial institutions within their relevant jurisdictions has fallen short of expectations. Overseers have stressed the importance of this entire initiative and will continue to monitor the actions required to improve the supervisory onboarding and safeguard the effectiveness of the KYS application.

As per standard procedure, overseers contributed, together with the national member groups, to the yearly review of the Customer Security Control Framework (CSCFv2023), which resulted in one advisory control being turned mandatory, as well as a number of other changes to the framework:

i. Promotion of the "advisory" control "1.*5 A Customer Environment Protection*" to "mandatory", with the objective of further aligning Swift's different architecture types, as well as protecting all connectors within different architecture types consistently;
ii. Introduction of a lighter attestation regime for Receiving-Only users. Over 1 100 active BICs have been identified by Swift as only receiving files or messages, not emitting any (potentially fraudulent) messages. Examples are corporates using reporting or dashboard applications. For these users, the recurring CSP compliance with Independent Assessment has become a costly annual exercise while representing minimal risk to process fraudulent transactions. This is why Swift proposes a lighter version of the CSP for Receiving-Only users. The requirement for this is that users will have to declare being a Receiving-Only institution, after which Swift will centrally implement controls to prevent any message or file being sent from their BICs. After this procedure, the user in question will still have to provide an annual attestation but will be exempt from the Independent Assessment.
iii. The method of indicating compliance to the CSCF has been simplified to bring it in line with other security frameworks and industry practices. Institutions and participants can now indicate compliance by checking a single check box, with the option to include written comments in a text box.

Swift users are expected to comply with the mandatory security controls (i.e. security baseline) and can also attest their compliance with the advisory controls (i.e. good practices for securing local IT infrastructures). A user's self-attestation (i.e. compliance with the CSCF security controls) is uploaded to the Know-Your-Customer Self-Attestation (KYC-SA) tool by the end of each year. The new CSCF version (v2023) was introduced in mid-2022, and users have until the end of 2023 to submit their attestations.

By 31 December 2022, 87 % of Swift customers had provided a valid CSP attestation, and of these self-attestations 79 % of customers indicated compliance with all mandatory controls. The compliance levels and the number of self-attestations are in line with the uptake in 2020 and 2021. Through Swift's quality assurance and monthly metrics reports, overseers closely monitor various CSP-related metrics, such as the users' attestation and consultation levels. The reporting on CSP metrics is crucial for overseers to obtain a view of the cybersecurity stance of the Swift user community. As such, overseers expect Swift to refine and extend the CSP reporting metrics as appropriate.

The Independent Assessment Framework (IAF), which was launched in mid-2021, requires all Swift users to perform a Community Standard Assessment to further enhance the accuracy of their attestations. Every Swift user has to have their attestations independently assessed through either an internal independent assessor (e.g. the second or third line of defence) or by an external independent assessor (such as a consultancy firm). Users are free to select the internal and/or external resources to conduct the assessment. If a user still opts for a self-attestation without the independent internal or external assessment; they will be considered as non-compliant to the CSP.

Initial reporting on compliance to the IAF looks promising, with 96 % of users indeed opting for an independent assessor, and thus remaining compliant with CSP requirements. Of these users, about half opt for an independent internal assessor, while the other half opts for independent external assessors. The percentage of Swift traffic sent by BICs who provide attestations supported by an independent internal assessment or an independent external assessment is fairly constant at 99 %.

Overseers also assess Swift's processes for communication with its users regarding the use of new technologies, fraud cases, and common cyber security threats affecting the community. Swift's Information Sharing and Analysis Centre (ISAC) provides its users with actionable information on cyber threats, indicators of compromise and common hacking practices. For example, through the ISAC portal, Swift shares relevant information on the Log4j vulnerability and the actions Swift users should undertake. The timeliness and comprehensiveness of the information sharing on such events is also covered by the overseers' review.

4.2.4 ISO 20022 migration

In close cooperation with its user community, Swift has been in the process of developing and testing ISO 20022, a richer and standardised information which is intended to promote greater transparency and speed, and lower cost for cross-border payment transactions. Swift originally planned to initiate the migration phase in November 2022. This launch date has been postponed, due to requests from the user community. At the end of 2022, the European Central Bank announced that it would delay the ISO 20022 migration within the Eurosystem by four months. Upon this announcement, Swift followed a community request to postpone the start of the cross-border ISO 20022 to March 2023 to align the start of the global ISO 20022 migration for CBPR+ with the ECB's updated timetable to ease implementation. This co-existence period, during which users will be expected to switch from the legacy FIN MT to the new ISO 20022 MX format, will thus start in March 2023 and end in November 2025.

Nothing prevents individual users to already exchange ISO 20022 messages sooner than this revised launch date. Since August 2022, all required capabilities have been deployed and institutions have been able to exchange ISO 20022 messages for CBPR+ on an opt-in basis. As such, institutions wanting to realise the benefits of ISO 20022's rich data format for CBPR+ sooner than March 2023 can continue to exchange ISO 20022 messages on an opt-in basis.

As a global standard-setter, Swift takes the lead in coordinating the ISO 20022 migration for its community. From the beginning, overseers have closely monitored Swift's approach, project management and planning, risk assessment, and communication with users. A recent development that Swift announced was the launch of the in-flow translation service, which will be made available for testing before the migration starts, and enables receipt of both FIN MT and ISO 20022 MX messages. With this service, Swift wants to make sure that participants can switch at their own pace during the co-existence period until November 2025. Overseers have closely analysed the scope and testing of the service. On Swift's side, everything has been brought up to readiness to support the global migration of the financial community to ISO 20022 by March 2023.

BOX 10

Impact of sanctions on Swift

The Russian Federation's invasion of Ukraine in February 2022 has had profound and cascading effects on geopolitical relations and the global economy. One of the measures taken in consequence was the European Commission's various sanctions packages targeting entities in or affiliated with Russia or Belarus. Included in these packages is the prohibition to provide specialised financial messaging services to the banks specifically listed in the sanctions decisions. As Swift is under EU and Belgian jurisdiction, in order to remain compliant with European laws and regulations, Swift was required to disconnect those Russian and Belarusian banks from its financial messaging network falling under applicable council regulation.

In order to be continuously in compliance with European laws and regulations, Swift is expected to keep track of changes in the ownership structures of its users, as any legal person, entity or body established in Russia or Belarus whose proprietary rights are directly or indirectly owned for more than 50 % by a sanctioned entity will also become a sanctioned entity by operation of law and should be disconnected from Swift's financial messaging network accordingly.

As pointed out in section 2.1, Swift FIN traffic growth in 2022 was slightly lower than in previous years, in particular for payments. One of the explanatory factors is the traffic lost because of the disconnection of sanctioned banks, next to the reduced interactions with Russia and Belarus triggered by sanctions overall. Year-end figures for 2022 show that Swift FIN traffic sent/received by Russia declined by 56 % and 61 % respectively; for traffic sent to / received from Belarus, the decrease was 50 % and 52 % respectively. This fall in traffic only kicked in as of March/April 2022, following the Russian invasion of Ukraine and the ensuing establishment of sanctions.

4.2.5 Transaction Management Platform

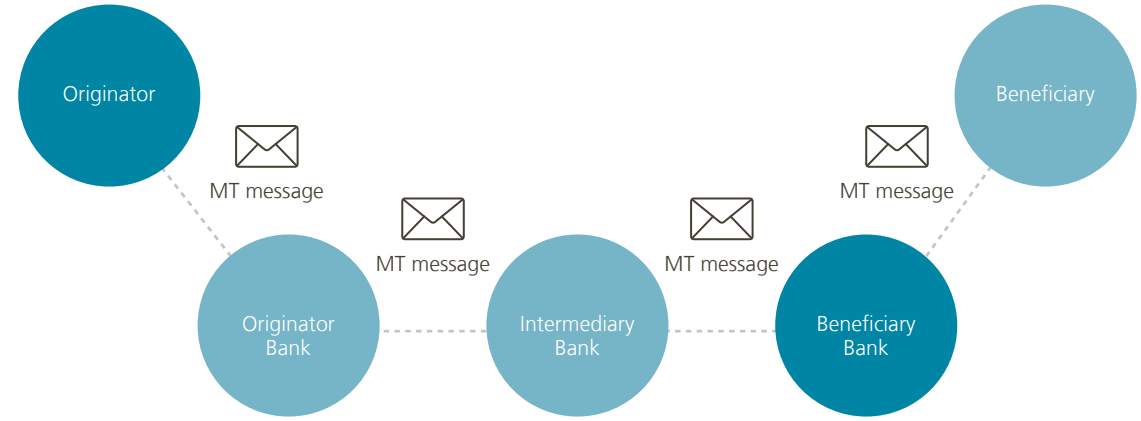
In 2019, Swift revealed their plans to build the Transaction Management Platform (TMP), moving away from traditional sequential messaging to an orchestrator which allows every single participant within a transaction to have an end-to-end and up to date view on the status of the transaction. Swift's Transaction Manager has been deployed live since November but has not yet been processing live customer traffic. Traffic build-up will start from the end of May 2023 until the end of September 2023. The move from FIN MT to ISO 20022 MX is not dependent on the activation of the TMP.

As the following figure illustrates, Swift's current message flow consists of MT messages forwarded from originator to beneficiary using Swift's secure communications channel. Swift's processing is message-driven and there is no central notion of the end-to-end transaction generating the underlying messages between all parties involved.

By evolving from secure message forwarding to end-to-end transaction management orchestrated by TMP, Swift wants to use richer data and reduce friction (i.e. provide better customer experience, increased efficiency, and new value-added services such as transaction validation). The following figure shows that the underlying communication channel for a transaction is format agnostic and could be FIN MT, ISO 20022 MX or Application

Figure

Current sequential Swift message flow

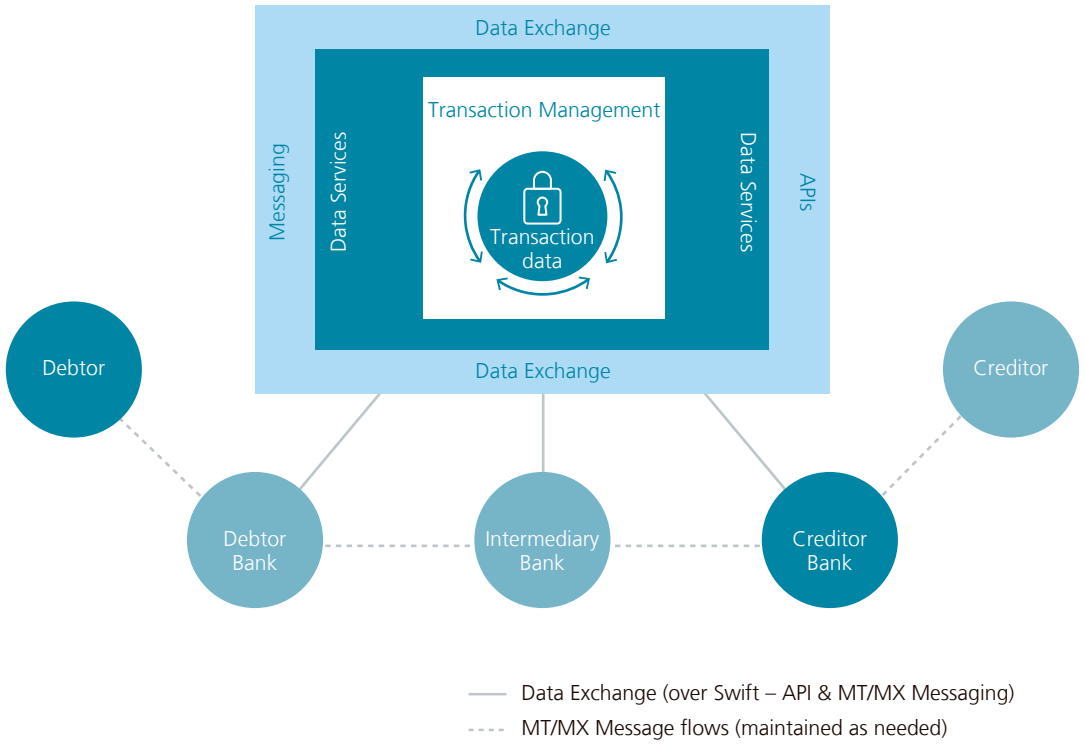


Source: Swift.

Programming Interfaces (APIs), or a combination of channels based on the capabilities of the transaction parties involved (i.e. backward compatibility). The platform maintains full transaction data accessible to any authorised party in the transaction chain, helping to ensure end-to-end transparency. TMP in future could also facilitate the use of APIs so that authorised users can retrieve the transaction status via an API call over the Swift network.

Figure

Planned end-to-end Swift transaction flow



Source: Swift.

TMP has a major impact on Swift's core messaging operations since it changes the payment message flow approach. Therefore, overseers have repeatedly conducted thorough reviews to obtain a complete picture of all relevant HLE aspects of TMP: analysis of risk assessments and corresponding mitigating actions, security and resilience features of the platform, architectural blueprint, project management, customer communication and engagement initiatives. Since TMP touches upon all five HLEs, the project has been part of the continuous oversight monitoring activities. Despite Swift confirming project delivery within the revised timeframe by the end of May, with the first full-scope version forecasted to roll out by September 2023, overseers will continue their critical and risk-based review of the project throughout 2023 and after its launch.

4.2.6 Faster payment initiatives

Launched in 2017, Swift global payments initiative (gpi) has gained momentum as the new standard for cross border, large value payment transactions. Swift gpi combines the traditional Swift messaging and banking system with a new set of rules. Any financial institution joining gpi has to follow these rules, which include transparency of fees, end-to-end payment tracking, and confirmation of credit to the recipient's account. Each transaction is assigned a Unique End-to-End Transaction Reference (UETR) that payment providers can use to trace the transfer from start to finish.

The benefits for customers joining gpi are numerous. First of all, gpi substantially increases payment speed. It eliminates payment friction and reduces the risk of delays through upfront account verification. Another way gpi reduces friction is through automated exception management processes, enabling users to easily handle queries between banks on the Swift network and resolve instances when payment information is incorrect or missing.

Another important dimension from the viewpoint of participants in cross-border transactions is financial crime compliance. Gpi offers a portfolio of financial crime compliance solutions that help member institutions to navigate more complex compliance requirements.

Gpi perfectly fits into Swift's strategy for fast and frictionless messaging services. As the benefits of gpi are realised leveraging the existing Swift messaging infrastructure, users can expect the same level of security and resilience as is the case when using traditional Swift messaging services.

Whereas Swift gpi facilitates high-value or wholesale cross-border payments, Swift Go aims to deliver on the strategy of fast and frictionless payments for low-value international payments. Introduced in July 2021, Swift Go is an interbank service that makes it quicker and cheaper for participating banks to send low value cross-border payments, with the possibility of instant settlement. It enables sending banks to fully customise their front end to offer an easy and intuitive payments experience to their customers. As such, Swift wants to ensure that the traditional banking sector remains competitive in the high-growth market of low-value cross-border payments.

Swift Go uses the Swift gpi rails to deliver speedy cross-border payments. It leverages enhanced service levels between banks, a single payment format and pre-validation services, ultimately removing delays caused by frictions in the transaction chain. In addition to faster payments, Swift Go offers more competitive processing fees, additional transparency, predictability, and payment tracking, combined with the security that users have come to expect from Swift. More than 400 customers have signed up for Swift Go, covering more than 110 countries. Of those, more than 60 banks were live by the end of 2022[1].

Both these services, which are gaining momentum and global reach, demonstrate Swift's continued commitment to delivering on the company's strategy of fast and frictionless payments for its global user community. The products have been repeatedly reviewed by overseers on their functionality, interaction with core messaging services, security aspects, proposed enhancements, and adoption rates.

1 Swift Go: The new standard in low-value international payments, Sibos 2022 in Amsterdam.

BOX 11

Swift's innovations with regard to CBDCs and tokenised assets

As well as trying to solve current challenges on the payments and securities markets, Swift is also looking ahead at the future. With the emergence of innovations such as Central Bank Digital Currencies and tokenized assets, Swift is assessing the role it could play to counteract the potential fragmentation in financial markets caused by these innovations becoming mainstream technologies.

To this end, Swift has set up experiments demonstrating the capability to leverage its existing infrastructure to handle CBDCs and tokenised assets on existing financial infrastructure. This is seen as a major milestone towards enabling their smooth integration into the international financial ecosystem.

At the time of writing, 114 countries, representing over 95 % of global GDP, are exploring a CBDC [1]. They often use different technologies, with primary focus on domestic use. For the potential of CBDCs to be fully realised across borders, these digital currencies need to overcome inherent differences to interact with each other, as well as with traditional fiat currencies.

In collaboration with Capgemini, Swift has made CBDC-to-CBDC transactions between different DLT networks based on popular technologies, as well as fiat-to-CBDC flows between these networks and a real-time gross settlement system. This success showed that the blockchain networks could be interlinked for cross-border payments through a single gateway, and that Swift's new transaction management capabilities could orchestrate all inter-network communication.

Numerous central and commercial banks are collaborating in a testing environment to speed up the path to full-scale deployment.

In a separate experiment with a different group of participants, Swift has similarly demonstrated that its infrastructure can serve as an interconnector between multiple tokenisation platforms and different types of cash payment.

Working in collaboration with many private companies, Swift last year explored 70 scenarios simulating market issuance and secondary market transfers of tokenised bonds, equities and cash. It successfully served as a single access point to various tokenised networks and showed its infrastructure could be used to create, transfer and redeem tokens and update balances between multiple client wallets, as well as providing interoperability between different tokenisation platforms and existing account-based infrastructure.

1 Atlantic Council, Central Bank Digital Currency Tracker, available at https://www.atlanticcouncil.org/cbdctracker.

The World Economic Forum has estimated that the tokenisation market could be worth $ 24 trillion by 2027[1]. Tokenisation has great potential when it comes to strengthening liquidity in markets and increasing access to investment opportunities, and Swift's existing infrastructure can ensure these benefits can be realised at the earliest opportunity, by as many people as possible.

As is the case for the introduction of Swift gpi and Swift Go, these experiments are part of Swift's extensive innovation agenda in support of its strategic focus on enabling instant, frictionless and interoperable cross-border transactions.

1 HSBC, The 10x potential of tokenisation – Democratising investment opportunities, available at https://www.gbm.hsbc.com/-/media/gbm/insights/attachments/potential-of-tokenisation.pdf.

4.3 Focal points for oversight in 2023

The annual planning of Swift oversight is driven by a risk-based approach. The oversight risk assessment helps to maximise the effectiveness and efficiency of the review activities. The assessment of the work in 2022 feeds into the 2023 planning. After each quarter, overseers look into the topics analysed and decide which ones require deeper review, or the items for which Swift needs to provide additional information. This approach creates sufficient flexibility for overseers to dedicate more time to certain topics when needed, or to hold a follow-up discussion at a later stage.

Swift operates in a changing environment with ever fiercer competition and rapidly evolving technologies. That context affects Swift's go-to-market strategy (e.g. agile software development) and operations (e.g. incident management), and poses additional challenges, such as geopolitics, the global scarcity of skilled resources and the changing cyber threat landscape. Overseers are aware of the pace of change and will continue to monitor how it affects Swift in terms of technology planning, resilience guarantees, risk assessments, security decisions and design choices, while keeping users properly informed. At all times, overseers seek assurance that the identified risks arising from new technology choices and major projects are adequately managed and mitigated, to ensure business continuity with comparable or better resilience.

The cyber security strategy and management of risks also remains a major topic on the overseers' agenda for 2023. Overseers analyse which security investment and enhanced capabilities will contribute to Swift's protection against more sophisticated cyber attacks. The cyber security review also involves challenging the ISAE3000 reports conducted by Swift's external security auditor. These reports provide independent assurance on Swift's internal control policies, procedures and controls structured around the five HLEs. The ISAE3000 reports consist of valuable information of importance to the oversight on Swift and are thoroughly reviewed each year.

The follow-up on CSP is also part of the oversight activities for 2023. Overseers will take a closer look at the supervisory involvement and the improvement measures that Swift takes, the CSCF review, the outcome of the first independent assessments, CSP metrics and further refinements, the Swift user community's level of compliance

with the CSCF controls, developments concerning customer cases, results of the new cycle of mandatory independent assessments, and other relevant CSP initiatives and campaigns. In its capacity as lead overseer, the National Bank of Belgium will also hold an outreach session with the Swift Oversight Forum to provide an update on the proposed changes to the CSCF. In doing this, the NBB urges other national authorities to keep pushing their institutions under supervision to improve their endpoint security, as well as for authorities and supervisors to leverage the capabilities of the Know-Your-Supervisor Self-Assessment data within their oversight toolbox.

In 2023, overseers will also aim to get better insight into the broader area of third-party risk management (TPRM) and supply-chain risk management. The distributed and interconnected nature of information technology products and services, and the potential risks that this might pose to financial market infrastructures, has been gaining attention over recent years. Diligent management of exposures to cyber security risks throughout the supply chain and guarding against threats and vulnerabilities among third-party suppliers or their products and services is the main goal of TPRM. This already was a recurrent topic within Swift oversight, but will be given renewed focus during 2023.

Two large projects – TMP and ISO 20022 migration – will reach their delivery deadline in 2023. Overseers have already conducted recurring and thorough reviews of these two projects but will continue to do so during 2023, with stronger focus on the final preparations before launch and communication with customers.

Another area covers major standing topics such as interactions with the risk department and internal audit. Each review cycle includes a dedicated touchpoint with the second and third lines of defence (LoD) to gain a clear understanding of their activities and obtain their views on certain projects and developments at Swift. Following the on-site reviews (OSRs) of the second line of defence (2018) and of the first line of defence (2020), overseers decided to conduct such a review on the third line of defence in 2022. The on-site review resulted in the opinion of overseers that Swift complied with the Institute of Internal Auditors' International Professional Practices Framework (IPPF), which forms authoritative guidance for internal audit professionals worldwide. The results of this review have been shared with Swift, and for those areas where further improvements were suggested by the OSR team, overseers will follow up with Swift throughout 2023 on the status of implementation of these improvements. Another OSR will be performed in 2023, demonstrating the success of this form of collaborative oversight, and leveraging the expertise from other central bank participants to focus on any particular domain for which overseers want to gain additional assurance.

The oversight planning for the following year is structured around the five HLEs which form the starting point for selecting topics for review. Following a risk-based approach, the previous year's assessment forms the basis for the review activities of the coming year. For 2023, this resulted in an extensive set of topics to be analysed by overseers, of which the following are a sub-set:

- HLE 1 Risk Identification and Management
  - Operational impact of the pandemic;
  - Internal and external audit findings;
- HLE 2 Information Security
  - Cybersecurity roadmap;
  - Customer incidents and forensic capabilities;
- HLE 3 Reliability and Resilience
  - Business continuity exercises;
  - Impact of technological developments on Swift's resilience;
- HLE 4 Technology Planning
  - Financial Crime Compliance portfolio;
  - Transaction Management Platform & ISO 20022 migration;
- HLE 5 Communication with Users
  - Customer communication related to ISO 20022 migration;
  - Customer adoption plans.