
Annual Review

# 2017

**Moving fast: Efficiency without compromise**

## Contents







**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 and standards for communicating, and we offer products and services to facilitate access and integration, identification, analysis and regulatory 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. While SWIFT does not hold funds or manage accounts on behalf of customers, we enable our global community of users to communicate securely, exchanging standardised financial messages in a reliable way, thereby supporting global and local financial flows, as well as trade and commerce all around the world.

As their trusted provider, we relentlessly pursue operational excellence; we support our community in addressing cyber threats; and we continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Our products and services support our community’s access and integration, business intelligence, reference data and financial crime compliance needs.

SWIFT also brings the financial community together – at global, regional and local levels – to shape market practice, define standards and debate issues of mutual interest or concern.

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.

## 2017 highlights

**SWIFTNet availability**

**99.999%**

**FIN availability**

**99.999%**

**Services exceeded availability targets**

**100%**

**Institutions connected to SWIFT**

**11,000+**

**Countries and territories**

**200+**

**Total FIN messages**

**7.1 billion**

**Average daily number of FIN messages**

**28.1+million**

**Fin messaging peak day**

**32.8+million**

**FIN growth**

**+8.4%**

**Total FileAct traffic (Kchar)**

**5.0+billion**

**Average daily FileAct traffic (Kchar)**

**20.2+million**

**FileAct growth (Kchar)**

**20%**

**Total InterAct messages**

**2.1+billion**

**Average daily InterAct messages**

**8.6+million**

**InterAct growth**

**+85%**

# Chairman's letter

**Yawar Shah**
Chairman of the Board

**SWIFT and the financial community made significant progress this past year in strengthening the industry's cyber defences against a threat that continues to evolve and aggressively targets the financial sector. At the same time, SWIFT continued to meet its service obligations and ensure the smooth running of its business day-to-day. Operating and financial performance was consistently strong throughout 2017, and excellent progress was made towards meeting the community-endorsed *SWIFT2020* strategic objectives.**

SWIFT continued to evolve its commercial offerings in 2017, launching successful new products that are significantly improving the correspondent banking experience for customers worldwide. The global payments innovation (gpi) has gone from strength to strength, continuing to attract new participants and impressing customers with its speed and efficiency. The Financial Crime Compliance portfolio continued to grow to cover more requirements as the need for efficient compliance processes becomes ever more important.

Through the Customer Security Programme (CSP) SWIFT provided tools, information and advice to help the community secure the perimeter, as well as mandatory and advisory controls which had to be implemented within an aggressive timeline. By year end, 89% of customers had attested to their level of compliance with the mandatory security controls. This outstanding result, which accounted for more than 99% of all cross-border traffic sent over the SWIFT network, is testament to the hard work of both SWIFT and the community in tackling the cyber threat head on.

It is vital that customers re-attest their full compliance of the mandatory controls by the end of 2018. Furthermore, global transaction banks should begin to use the wealth of attestation data that is now available to them. Consulting the KYC Security Attestation (KYC-SA) application to see which of their customers and counterparties have attested, requesting access to that data and then consuming and acting on it with a risk-based framework, will be essential in helping banks to assess relationships more effectively and thereby better manage counterparty risk.

Cyber security is, of course, not the only challenge facing our community. Customers are demanding faster payments and greater transparency; regulators and banks want to prevent the sector being used to facilitate criminal activity and terrorism, but are concerned about de-risking; and competition from FinTechs and powerful incumbents continues to grow – a combination which is challenging correspondent banking in a number of areas. All this requires SWIFT to continue ensuring its operational reliability, security and effectiveness, while at the same time doubling-down on building on the success of gpi, the CSP and its financial crime compliance portfolio.

Over the course of 2017 SWIFT has reinforced its role as a provider of FinTech solutions to both the payments and securities industries. Now is the time for SWIFT to further accelerate its efforts for the benefit of the communities it serves. That includes enhancing and extending gpi, while continuing the momentum of the other business initiatives.

In addition, SWIFT will continue to leverage its unique position and skills, incorporating new and maturing technologies and trends where relevant. Application Programming Interfaces (APIs) are fast emerging as a way for financial institutions to expose services to end customers and to each other. Driven by regulation designed to promote competition, such as Open Banking and PSD2, banks are on a steep learning curve to master and deploy this technology.

But whatever the technology, in a network business like financial services, familiar challenges remain: securing infrastructure; gaining efficiencies and reducing risk through standardisation; ensuring platform resilience and scalability to meet future needs. Rest assured that SWIFT has these issues in its sights and in 2018 it will continue to develop its core competencies in technology and standardisation to address them on your behalf.

Turning to standards, for over 40 years the SWIFT MT standard has enabled industry automation, reducing the cost and risk of cross-border business, and enabling the development of a correspondent banking system on which world trade depends. While MT continues to be maintained in line with users' needs, in recent years SWIFT has worked to develop and promote ISO 20022, a more modern standard with significant functional and technical advantages. SWIFT has initiated an industry consultation, endorsed by the Board, to capture key facts about the community's readiness and appetite for migration, identify the obstacles to be overcome, and propose a migration strategy to enable all users to make the transition.

The SWIFT Board is determined to ensure that your cooperative is agile in supporting your commercial businesses, and I know SWIFT management and staff are committed to innovating and developing solutions that bring added value to the community, while ensuring operational excellence and security.

I would like to thank my fellow Board members for their commitment to and continued guidance of SWIFT to ensure it does not lose sight of its 'true north'. SWIFT's governance is strong, and provided by a broad-based and talented group of Board members. I thank the SWIFT management team and staff for another year of leadership, hard work, dedication, and perseverance in bringing value to the community.

As Board Chairman, I am honoured to serve the community, and I thank you for your support.

**Yawar Shah**
Chairman of the Board
May 2018

# CEO's letter

**Gottfried Leibbrandt**
CEO

**2017 was a pivotal year for SWIFT and our community. The unparalleled challenge of the cyber threat, in combination with the urgent need to innovate in an increasingly competitive environment, left no room for complacency.**

In January, we brought a new payments experience to life with the top global transaction banks going live with global payments innovation (gpi), a capability that enables banks to give their customers a much enhanced cross-border payments experience through real-time tracking, greater transparency on fees and radically increased speed. By the end of the year, gpi banks were sending over $100 billion every day using SWIFT gpi across 220 country corridors, with 50% of payments credited in less than 30 minutes. Over 150 financial institutions had signed up to gpi by the end of 2017, and before the year end we announced plans for added features such as the ability to stop and recall suspicious payments, along with the inclusion of rich text data to improve the information available in a specific payment instruction.

At the same time, we continued to work with our community to increase cyber security through our Customer Security Programme (CSP). An overwhelming majority of customers had attested against the CSP controls by the year-end deadline, a clear demonstration of the community coming together to up its game against the threat. We also saw a steady increase in the use of the SWIFT Information Sharing and Analysis Centre (SWIFT-ISAC) that launched in May. We published 65 bulletins that were consulted more than 38,000 times by more than 3,100 institutions. And together with a world-leading cyber security company, we co-authored a report for our customers to learn about the evolving techniques and tactics used by those who seek to harm our community.

We continue to support our community in fighting against the evolving cyber threat by investing in and developing new tools: for instance, our Payment Controls Service, set to go live in 2018, will enable subscribers to check their outgoing messages on the SWIFT network in real-time against specific user-selected criteria, thus detecting any unusual message flows before transmission.

Our Financial Crime Compliance (FCC) portfolio continued to see wide adoption, with more than 4,500 financial institutions from 200 countries registered on the KYC Registry to date. We also witnessed a significant acceleration in users downloading counterparty information. In addition, more than 800 users registered to our Sanctions Screening Service and in December we launched the batch version of our name screening service. These services play a significant role in addressing industry-wide challenges while reducing cost, complexity and risk for all of our customers.

With the combination of gpi, the CSP and our FCC solutions, the SWIFT community is creating a new transaction banking paradigm, founded on principles of speed, transparency, security, compliance and trust. By innovating from the core, building on our strengths, and developing new innovative solutions based on the latest technologies, we are in a strong position to compete and collaborate in the growing FinTech ecosystem.

While developing new technologies and services with our customers, we continued to deliver high service levels in 2017 with FIN traffic rising to an all-time high of 7.1 billion messages; this was fuelled by a double-digit growth in payment volumes. While SWIFT's FIN traffic grew by 9% over the year, FIN Payment traffic rose by 12%, driven by growth across all regions and the adoption of our gpi service.

SWIFT continued to deliver on its day-to-day mandate: operational availability performance during 2017 exceeded targets. SWIFT achieved 99.999% availability both for FIN and its SWIFTNet messaging services, against the backdrop of growing volumes and technology renewal.

While much effort went into transaction banking, we also made further progress in expanding our Market Infrastructure presence, for example with the New Payments Platform (NPP) in Australia up and running by the end of the year. Furthermore, we announced that from November 2018 SWIFT will supply connectivity to the European instant payments system TIPS and the EBA's pan-European RT1 platform, bolstering our involvement in Instant Payment solutions.

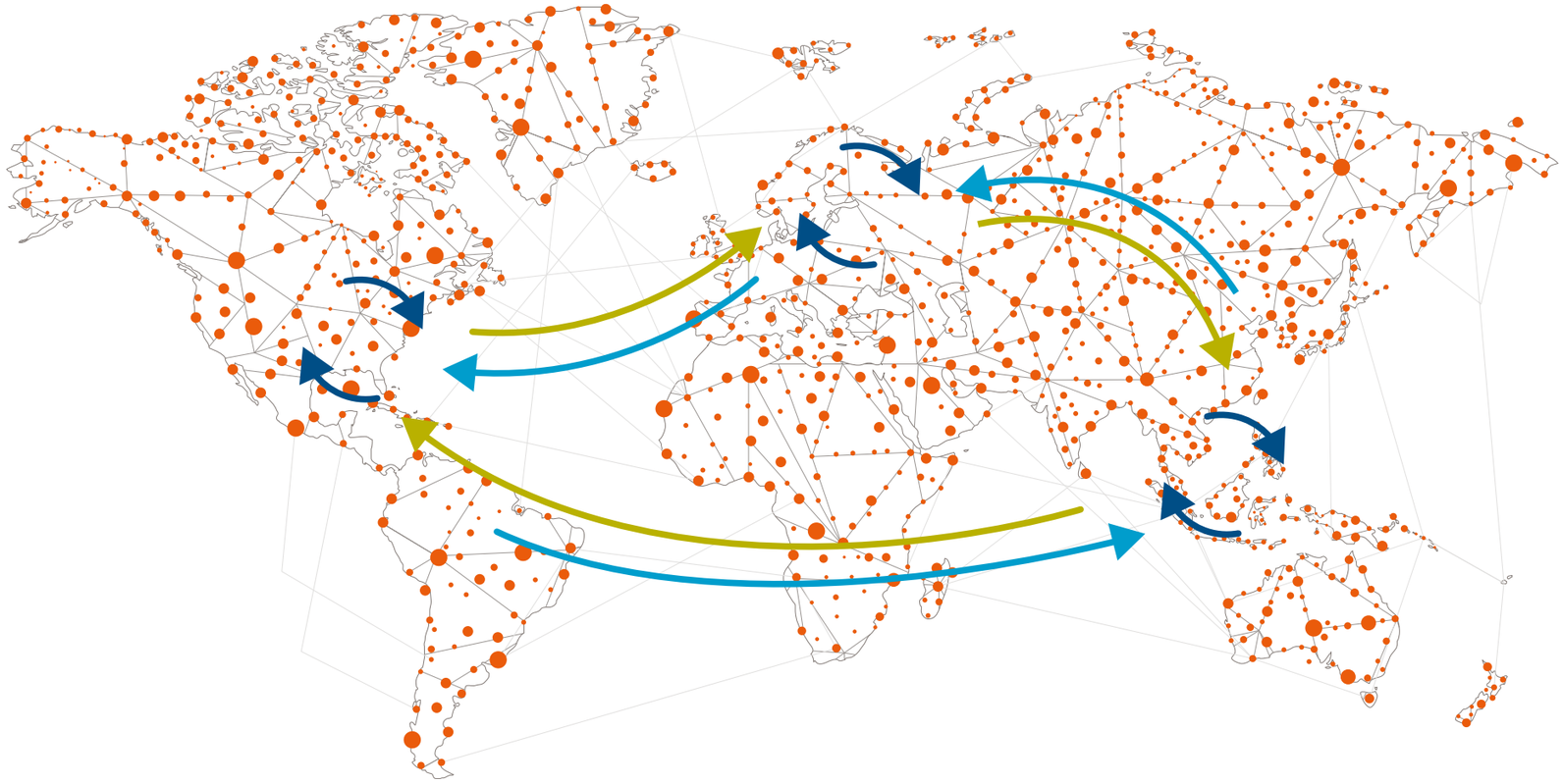
And we are already laying the foundations for further innovation by exploring new technologies. SWIFT completed a landmark Distributed Ledger Technology proof of concept (PoC) with 34 banks; making it one of the most extensive Hyperledger Fabric technology implementations in the industry to date. While successfully meeting all the business requirements that had been set out, the PoC evidenced that there are considerable pre-requisites for such a solution to be adopted by the industry at scale. We will continue to explore use cases with our community in the SWIFT DLT Sandbox and are keen to see this technology mature.

2017 has been a year to look back on with pride. I want to put on record my warm thanks and gratitude to all the SWIFT staff who have helped deliver so much last year and I go forward, confident in the knowledge that they will carry on doing so.

It has certainly been a year in which SWIFT has stepped up to the challenge and I appreciate the Board and the community's continued support and guidance.

**Gottfried Leibbrandt**
CEO
May 2018

# Payments regional traffic flows



**2017 average daily FIN payments volume (in Kmsgs) and growth versus 2016**

This traffic compares year-on-year growth rates for regional payment flows in 2017. SWIFT observed traffic growth in all regions and for all routes between regions. While EMEA intra-region payments traffic represents the highest share of the volume, strong intra-regional traffic growth was recorded in all three regions.

## Americas

Sent: 2,942 Kmsgs (+12.5%)
Received: 2,719 Kmsgs (+ 9.2%)

**Intra-Americas:** 1,277 Kmsgs (+10.7%)
**Sent to Asia Pacific:** 627 Kmsgs (+14.5%)
**Sent to EMEA:** 1,038 Kmsgs (+13.4%)

## EMEA

Sent: 6,616 Kmsgs (+10.3%)
Received: 6,701 Kmsgs (+10.9%)

**Intra-EMEA:** 5,290 Kmsgs (+10.8%)
**Sent to Asia Pacific:** 309 Kmsgs (+7.4%)
**Sent to Americas:** 1,017 Kmsgs (+8.6%)

## Asia Pacific

Sent: 1,536 Kmsgs (+8.5%)
Received: 1,674 Kmsgs (+11.9%)

**Intra-Asia Pacific:** 738 Kmsgs (+11.7%)
**Sent to EMEA:** 373 Kmsgs (+5.4%)
**Sent to Americas:** 425 Kmsgs (+5.9%)

Figures are based on user-to-user live payment traffic.

# Operational performance

**In 2017, SWIFT continued its focus on reliability and security, resulting in 'five nines' availability for both FIN and SWIFTNet messaging services. This achievement is impressive given that it occurred against a backdrop of increasingly sophisticated cyber threats, and strong traffic growth.**

On 30 November 2017, SWIFT recorded a new peak day, with 32,839,705 messages sent over the FIN network. Being the third peak day of the year, it was 5.9% above the previous peak day recorded at the end of October. SWIFT's total FIN traffic rose to an all-time high of 7.1 billion messages in 2017, compared to 6.5 billion messages in 2016.

**Cyber security – the bedrock of our community**

The ever-increasing sophistication of cyber attacks means we cannot be complacent. We continued to focus on improving the security of our customer footprint, implementing the 2017 cyber roadmap and building a strong security culture. Our IT and operations teams continue to work assiduously to further strengthen our monitoring capabilities and to assist our customers in implementing the local-user environments.

SWIFT's Customer Security Programme, which is designed to help banks protect themselves against cyber threats, continued to make good progress in 2017. In May, we introduced a set of security controls, some of which are mandatory, and asked customers to attest to their level of compliance with the mandatory controls by the end 2017. Compliance with the security controls continues to be an important undertaking for the industry and the resulting transparency will benefit everyone in terms of cyber risk management.

Our Security Operations Centre (SOC) provides rapid and effective real-time response to security alerts related to both the SWIFT production and enterprise environment, with a 24x7 security monitoring capability. Using the security tools, the SOC correlates logs and detects suspicious and malicious behaviour in these environments, including identification, containment and eradication of threats, and then escalates as needed. The current increase in the cyber threat has indicated the importance of effective cyber security measures with all entities involved in the processing of financial transactions.

In May 2017, SWIFT launched the SWIFT Information Sharing and Analysis Centre (ISAC) portal. The ISAC aims to facilitate the community's access to actionable cyber-security threat intelligence and enables the community to better defend itself against potential future cyber attacks. It is considered a highly trustworthy source for indicators of compromise.

In December 2017, SWIFT and cyber security specialists, BAE Systems, produced a detailed report on the evolving cyber threat, based on evidence gained from detailed forensic examinations from a range of recent cyber attacks on SWIFT customers. The report evidences the value of threat information sharing, and showcases how the resulting findings can be used to help protect against the cyber threat. The report is available to customers in the SWIFT ISAC.

**A track record of operational excellence**

Last year, SWIFT continued to invest in modernising its technology platforms to provide a better service to our community.

In February 2017, the final steps of the FIN Renewal programme were successfully completed. This programme, which was initiated in 2011, will increase our cost effectiveness and further strengthen scalability and resilience.

Several multi-year key initiatives have progressed in 2017, including, among others, the renewal of our Public Key Infrastructure, the Red Hat Linux server platform migration, and a complete renewal of SWIFT's back-office operations and tools. These evolutions use exciting new technologies such as containerisation, virtualisation and APIs, which are essential to our solutions, such as our global payments innovation, Instant Payments, and our Financial Crime Compliance portfolio.

With 500+ business continuity exercises in 2017, we continuously validated processes and trained our highly skilled staff to effectively handle a very broad range of disaster recovery scenarios, preparing them for any situation.

**Accelerating innovation**

Innovation is an integral part of SWIFT's DNA. We embrace open innovation by connecting with customers, startups, universities, vendors and innovation communities to capitalise on the wide range of emerging ideas and technology solutions. Through events such as hackathons and red team exercises we engage SWIFT teams across the organisation and foster our innovation mind-set.

Platform and business-driven innovation is a strategic enabler in providing products and services that serve our customers better. Examples of innovative initiatives that matured in 2017 include:

- SWIFT's global payments innovation (gpi) service, enabling end-to-end payments tracking, went live in January, followed by a full set of customer accessible APIs to obtain and update payment status. gpi Observer became available in May and the gpi Directory went live in September.
- We ramped up our activities around blockchain and Distributed Ledger Technology and deployed a Nostro Reconciliation proof of concept (PoC) on the DLT Sandbox to facilitate exploration with 30+ participants from the financial community. The initiative was one of the most extensive blockchain proofs of concept and Hyperledger Fabric implementations executed in the industry so far, both in terms of participant engagement and in terms of the scale of the infrastructure deployed. It demonstrated the significant progress DLT has made with regard to data confidentiality, governance, security, and identification frameworks, evidencing that the emergent technology, combined with SWIFT assets, provides the necessary foundation for financial multi-bank applications.
- Through the introduction of operational data mining and advanced analytics capabilities, we have started unfolding superior troubleshooting capabilities, such as 'out-of-pattern' behaviour identification.
- SWIFT announced that it would support the European banking industry and market infrastructures as they implement instant payments platforms. SWIFTNet Instant will go live in November 2018. SWIFT has also stated its commitment to the future Eurosystem Single Market Infrastructure Gateway, as laid out in the Eurosystem Vision 2020. SWIFT's instant payments solution will provide access to multiple instant payment operators in Europe and beyond, building upon SWIFTs contribution to the Australian New Payments Platform (AU-NPP), which was successfully delivered at the end of 2017.
- We continued to evolve our SWIFTRef portfolio towards corporates, with the launch of the Data Validation Service in 2017, aiming to help corporates to build and maintain accurate Master file in their ERP, to reduce payments errors and delays.
- SWIFT bolstered its securities markets business with the addition of FX Performance Insights, an unprecedented, fact-based and granular tool highlighting customers' businesses performance in the FX markets in comparison to their peers. FX Performance Insights provides customers with a unique, market-wide view, covering in excess of 8,000 customers across 130 currencies.
- SWIFT Translator was unveiled at Sibos 2017. Powered by MyStandards, SWIFT Translator is a message transformation tool that allows users to define and validate format translations from any format to ISO 20022 or MT.

**Continued focus on reliability, security and availability**

**Committed to operational excellence**

**Helping our community build a strong security culture**

**Delivering innovative products and services**

## SWIFT global payments innovation (gpi)


**The global payments innovation (gpi) – cross-border payments, transformed**

SWIFT, with its deep background and wealth of experience in cross-border payments, has a clear vision on the future of financial transactions and has harnessed this to increase the speed, transparency and end-to-end tracking of payments through our global payments innovation (gpi) initiative.

Established in 2016 to improve customer experience in cross-border payments, gpi made significant progress in 2017 with greater than expected take-up, following the introduction of an improved breadth of service and the leverage of several gpi-dedicated projects, including: the launch of The Tracker; a proof of concept (PoC) on DLT; and an Industry Challenge focused on the development of overlay services through APIs (Application Programming Interfaces).

By the end of 2017, over 140 leading transaction banks from four continents had signed up to gpi, with more than 100 billion USD in SWIFT gpi messages sent every day, and these figures continue to grow. Currently SWIFT gpi has been adopted by more than 150 financial institutions around the world and the resulting payments, which represent nearly 10% of SWIFT's cross-border payments traffic, are being sent daily across 220 international payment corridors. This includes major country corridors such as USA-China, where gpi payments already account for over 25% of the payment traffic.

In addition, more than 50 payment market infrastructures are already exchanging gpi payments, enabling domestic exchange and tracking.

In 2018 many more banks are expected to join and take advantage of the leading best practice and to benefit from the real world changes it brings about. To support this, our development work is staged over three phases, two of which began in 2017.

**Phase One**
The first phase of SWIFT gpi focuses on business-to-business payments, helping corporates grow their international business, improve supplier relationships, and achieve greater treasury efficiencies. With gpi, corporations can today receive an enhanced payments service from their banks, with the following key features:

- Faster, same-day use of funds
- Transparency of fees
- End-to-end payments tracking
- Remittance information transferred unaltered

**Phase Two**
The second phase, to be introduced in 2018, will realise the digital transformation of payments with a range of complementary services, such as stop and recall payments.

- gpi Stop and Recall – Allowing payment messages to be immediately stopped in case of fraud or error, no matter where they are in the gpi transaction chain
- gpi Universal Tracking – Enabling gpi banks to track gpi payments along the full payments chain, even when the banks handling the transaction have not yet adopted gpi
- gpi Cover Payment – Speeding up payment processing when there is no direct account relationship between the sender and receiver of a payment

**Phase Three**
For its third phase, SWIFT gpi is exploring the potential of using technologies such as distributed ledger technology (DLT) in the cross-border payments process.

In 2017, we launched a proof of concept to explore the potential of using DLT for the reconciliation of banks' nostro accounts, taking our initial findings to Sibos in October of 2017.

We also explored the potential of open APIs to support the third generation of gpi through an Industry Challenge event with 40+ customers and FinTechs selected from across the world, supporting our focus on further overlay services and a richer corporate customer experience.

**The gpi Tracker**
The gpi Tracker was launched in May 2017, representing the cornerstone of SWIFT gpi – combining real-time payments tracking with the speed and certainty of same-day settlement for international payments.

The gpi Tracker meets corporates' needs for greater visibility on their payments' status. It provides corporate treasurers with a real-time, end-to-end view of their payments combined with a confirmation notice when the money reaches the recipient's account. The Tracker also enables a more accurate reconciliation of payments and invoices, and optimises liquidity with improved cash forecasts. The Tracker is available via an open API, making it compatible with proprietary banking systems worldwide – helping to ensure maximum impact of gpi benefits at a greater adoption speed.





## Financial crime compliance

**Financial Crime Compliance is one of the most costly and complicated challenges facing the financial industry today. The techniques used by criminals and terrorists continue to develop and become more sophisticated, so regulators are raising the bar on banks' compliance requirements.**

At a time when financial crime compliance is critical to every institution operating in increasingly regulated financial markets, SWIFT is providing customers with the tools they need to address their sanctions, Know Your Customer (KYC) and Anti-Money Laundering (AML) requirements, as well as to combat fraud and cyber threats. These proven solutions in the compliance space address industry-wide challenges – in close collaboration with our customers.

Based on secure, hosted technology, shared services, industry defined standards and mutualised costs, customers are using SWIFT's compliance services to increase transparency, standardise processes, increase efficiency and mitigate risk.

At Sibos 2017, the compliance stream brought together senior compliance and business representatives to tackle current challenges and help define the way forward for the industry as a whole. Measurable objectives, improved skillsets, new technologies, risk-based strategies and increased information sharing were common themes. There was also a call for greater information sharing between banks, regulators and law enforcement agencies to support the shift to a more targeted, risk-based approach to financial crime compliance.

Also announced at Sibos, the newly formed Financial Crime Compliance Advisory Group will be tasked to ensure SWIFT product development priorities remain closely targeted on evolving client needs.

**In 2017:**

- SWIFT's initial compliance service – Sanctions Screening – surpassed 800 customers. At the end of 2017 we enhanced our hosted Name Screening service by adding batch screening to the online screening of single names. This offers an easier and more efficient way to screen the names of customers, vendors and other business relationship parties, and support sanctions compliance and customer due diligence.
- SWIFT's Compliance Analytics service surpassed 50 customers, representing over 75% of SWIFT message traffic. SWIFT added Correspondent Monitoring to its Compliance Analytics offering, providing banks with a truly unique look at correspondent banking, AML and correspondent risk.
- The KYC Registry exceeded 4,500 customer institutions, spread across every market where SWIFT is active. SWIFT aligned its 'KYC baseline' – the standardised dataset that member banks exchange using the Registry – with the new Wolfsberg Due Diligence Questionnaire – the de facto standard for correspondent banking due diligence.
- SWIFT launched Daily Validation Reports as part of its Fraud Solutions portfolio, with more than 70 banks signing up by year-end. This fraud risk mitigation tool represents a key deliverable in SWIFT's Customer Security Programme (CSP), and will be complemented by the launch of a real-time fraud detection capability, Payment Controls, in mid-2018.

## Customer Security Programme

**Helping customers secure and protect their local environment**

**Sharing detailed technical information with our community**

**Introducing products and services that provide additional safeguards**

**SWIFT's Customer Security Programme (CSP), launched in 2016, is designed to help customers implement the practices that are critical to help defend against, detect and recover from cyber crime. The CSP involves a layered defence, built from depth and designed to help our customers protect their local user environment from a range of threats.**

Customers have engaged very positively with the CSP since its roll-out and understand that the security of our community requires everyone's participation. This starts with each individual customer's own security.

In April 2017, we introduced the Customer Security Controls Framework, a set of security controls – 16 mandatory and 11 advisory – that set a security baseline for banks. The security controls were developed in conjunction with industry experts and designed to be in line with existing information security industry standards: PCI-DSS, ISO 27002, and NIST. They are kept under constant review to ensure our community is best protected from emerging and evolving cyber threats. Compliance with SWIFT's security controls is an essential step for customers towards securing their systems, and we asked customers to attest to their level of compliance with the mandatory controls by the end of 2017.

In the six months leading up to December 2017, SWIFT carried out a global engagement campaign to drive awareness and understanding of both the Customer Security Controls Framework and the attestation process. We held more than 200 dedicated customer security work sessions around the world, which were attended by more than 14,500 attendees. Engagement was reinforced through our business forums and regional events worldwide and via the regular National Member and User Groups meetings.

By the end of 2017, 89% of all SWIFT customers had attested their level of compliance with the mandatory security controls. Combined, these institutions account for over 99% of all FIN messages sent over the SWIFT network. The number of attestations continues to rise, as several hundred organisations have subsequently attested or have attestations in progress. This excellent response – across segments, markets and infrastructure types – demonstrates the financial industry's commitment to combatting the persistent threat of cyber attacks.

In 2017 your interface vendors also met the challenge to raise the bar on cyber resilience embedded or supported in their products. The Certified Interface Programme is designed to ensure that SWIFT interfaces developed by third parties meet stringent conformance and security requirements, including a set of mandatory and advisory security requirements which have been adapted from the Customer Security Controls Framework. Interface providers were requested to self-attest their compliance against the security controls by the end of December 2017 to qualify for interim certification and to be listed on the certification registry on swift.com. For an interface provider to qualify for full certification, a customer of their choice has to verify and confirm the interface provider's self-attestation. Interface providers must receive customer confirmation by mid-2018 to obtain full certification.

SWIFT's Alliance and SWIFTNet Release 7.2, which was made available in August 2017, provided a number of security enhancements and related features. In November 2017, we delivered the quarterly security update for our messaging and connectivity interface products. We will continue to provide security updates for SWIFTNet and Alliance products on a quarterly basis in 2018.

The security threat is, however, rapidly evolving and significant work will still need to be done to drive further security improvements and increase transparency across the financial community. All SWIFT customers will need to re-attest and to confirm full compliance with the mandatory security controls by the end of 2018, and attestations will have to be renewed annually thereafter. The Customer Security Controls Framework is built upon the principle of self-attestation and the transparent exchange of information between counterparties to allow customers to ascertain the level of their adherence to the controls. To ensure community transparency, SWIFT reserves the right to report those users who have yet to attest, to their financial supervisors, and customers have been reminded of this.

Customers should now begin to incorporate their counterparties' attestation data into their risk management and business decision-making processes – alongside other risk considerations such as KYC, sanctions and AML. Using the KYC Security Attestation (KYC-SA) application, which was launched in July 2017, customers are able to share their attestation data with their counterparties and request data from others. This creates an opportunity for an organisation to be transparent about their attestation status, which should increase the trust and confidence for counterparts doing business with each other.

Information sharing is hugely important in helping the industry to better defend itself against potential future cyber attacks, and SWIFT provides support through measures such as issuing security alerts, sharing anonymised information on Indicators of Compromise (IOCs), and detailing the modus operandi used in known attacks. The SWIFT ISAC global information sharing portal, launched in May 2017, is a channel for SWIFT to share detailed and technical intelligence with its community of users, to help the community protect itself, to take mitigating actions, and to defend against further attacks. The SWIFT ISAC now allows the automated exchange of cyber-threat information using industry-standard formats (STIX/TAXII).

In December 2017, SWIFT and cyber security specialists, BAE Systems, produced a detailed report on the evolving cyber threat, based on evidence gained from detailed forensic examinations of a range of recent cyber attacks on SWIFT customers. The report evidences the value of threat information sharing, and showcases how the resulting findings can be used to help protect against the cyber threat. The report is available to customers in the SWIFT ISAC.

We will continue to roll out new anti-fraud tools – for instance, our Payment Controls service, which will launch in Q3 2018, is an 'in-flight' service that provides real-time monitoring of payment messages sent over the SWIFT network and monitors payment messages in real-time in the SWIFT network. It will bring additional monitoring and reporting safeguards to ensure that payment instructions are in line with business expectations and don't represent a significant or an unacceptable business risk. Following the success of Daily Validation and based on requests from corporates, a new release allows users to access details of their MT101 messages. Finally, SWIFT's Relationship Management Application (RMA) plays an important part in supporting communication between different financial institutions. Against the backdrop of the current cyber threats, we continue to encourage institutions to review and clean-up RMA relationships and to consider the adoption of RMA Plus, which allows customers to specify which message types they want to receive from and send to their counterparties.

The priority for 2018 is for customers to confirm full compliance with the mandatory security controls. We continue to provide a lot of assistance to help customers with the attestation process. Support materials, such as Frequently Asked Questions documents, videos and webinar recordings, are available on swift.com, and customers can also consult the User Handbook, the SWIFTSmart training portfolio, mySWIFT, and Knowledge Based Tips for further advice and information. SWIFT has also published a directory of cyber security service providers that can provide further assistance with the attestation process.

# Market infrastructures

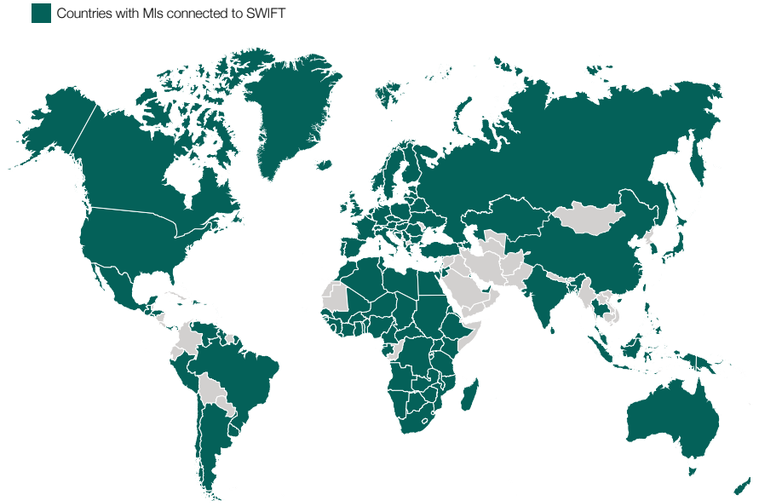
**SWIFT's Market Infrastructures (MI) franchise continues to contribute more than a third of SWIFT's total revenue and around 45% of our messaging volumes.**

This success is a result of our focus and investments in MIs, which is a strong driver for innovation at SWIFT. The traffic increase was driven in particular by the success of the T2S adoption. In November 2017 SWIFT delivered the real time 24/7/365 new payments platform in Australia that was made available to the public in early February 2018.

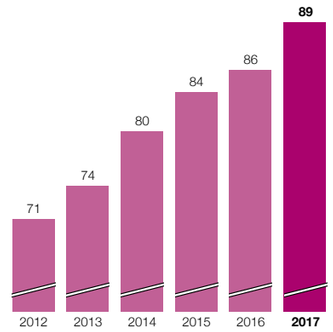
Building on this experience, SWIFT is developing an Instant Payments (IP) messaging solution focused on Europe which is planned to go live in November 2018.

We expect the MI segment to continue making a significant contribution in the coming years, in particular in the Instant Payments space. Because of the global adoption of ISO 20022, we see major shifts on the horizon for the very dynamic MI market segment, such as the planned renewals of many MIs across the payments and securities space. This rapidly changing business environment also creates an increasing need for resilience, which SWIFT intends to cover with its MIRS solution.

**136 countries with at least one market infrastructure connected to SWIFT at year end 2017**




**Central securities depositories (CSDs) connected to SWIFT**




**2017 figures**

HVP messages

**794million**

CSD and CCP messages

**2.9billion**

Live MI systems

**254**

Countries and territories with live systems

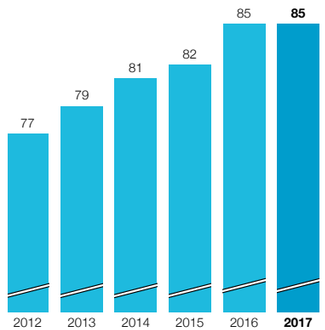
**140**

## Instant Payments

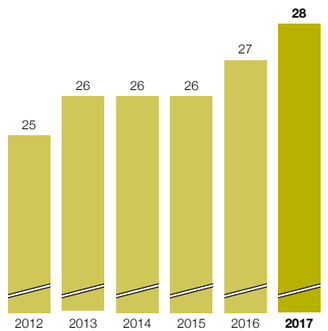
**The Australian New Payments Platform went live in November 2017 with SWIFT as the network and messaging provider**

**From November 2018 SWIFT will supply connectivity to the European instant payments system TIPS and the EBA's pan-European RT1 platform**

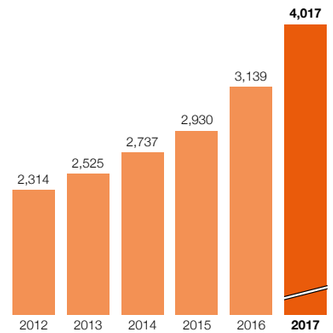
**High value payment (HVP) systems connected to SWIFT**




**Low value payment (LVP) systems connected to SWIFT**




**Number of messages sent and received by MIs on SWIFT**



# SWIFT worldwide

**SWIFT's events programme brought the global community together in 2017 at regional conferences, standards forums, business and operational forums. In the second half of 2017, we carried out the largest global engagement campaign in SWIFT's history. We organised more than 200 Customer Security Programme (CSP) work sessions worldwide, which were attended by 14,500+ attendees. Content was delivered to gear them towards self-attestation and compliance with the customer security framework.**

## Bringing the community together

## Debating topics of shared interest

## Showcasing innovative solutions and new thinking

### APAC

Business forums and regional conferences across nine countries gathered over 2,500 financial industry experts, where sessions focused on payments innovation, technological transformation, financial crime compliance, and cyber security. The forums were held in Singapore, Mumbai, Sydney, Beijing, Ho Chi Minh, Manila, Taipei, Tokyo and Seoul.

To close the year, SWIFT hosted the SWIFT gpi Industry Challenge in Singapore and, in two days, 50 gpi banks gathered with five FinTechs to collaborate and innovate on top of gpi rails. Two winners emerged and have progressed to develop Proof of Value for further community validation.

### EMEA

SWIFT welcomed 400 delegates from more than 45 countries at the African Regional Conference (ARC), which was held in Abidjan in May. Topics on the agenda included regionalisation, the future of payments, cyber security and financial crime compliance.

The SWIFT Business Forum London – SWIFT's largest regional event – took place in April and welcomed over 1,000 people. Leading figures from banking and industry discussed the dual challenges of how financial institutions can stay resilient and secure whilst continuing to innovate against a backdrop of uncertainty.

The Premium Services Forum Europe (PSF) and the SWIFT Operations Forum Europe (SOFE) took place at the end of November in Amsterdam. Under the theme Operations-Collaboration-Excellence, the two events brought together more than 500 operational experts from across EMEA to debate our industry's operational challenges and discuss how to achieve and maintain the levels of operational excellence and security we all aim for.

Business Forums in Sweden, Switzerland, Egypt, Russia, Benelux, Poland, Greece, France, East Africa, Spain, Romania and Austria looked at the key trends in each market and what SWIFT is doing to support local communities as they seek to turn challenges into opportunities. Many of these events also featured a SWIFT demo zone where customers could gain hands-on experience with our products and services and find out what SWIFT's R&D team is doing with new technologies such as Distributed Ledger Technology (DLT) and Artificial Intelligence (AI).

In addition to the regional conferences and business forums, we also held a series of other events in EMEA in 2017, including a dedicated SWIFT gpi day in Frankfurt, a Securities Day in Frankfurt, the Swiss Forum for Financial Standards and a Corporates Forum in Turkey.

### Americas

In March, SWIFT hosted the Business Forum Canada, which brought together 350 delegates in Toronto to discuss payment systems modernisation and the importance of continued collaboration on key issues such as cyber security.

In May, 400 delegates attended the inaugural SWIFT Business Forum Mexico – where the dual challenges of cyber security and compliance were discussed alongside innovation and financial inclusion.

The SWIFT Business Forum New York took place in June and brought together over 650 attendees. Senior figures from financial services and financial technology startups discussed the importance of working together in order to survive in a competitive landscape.

In June, SWIFT hosted the Premium Services Forum Americas in New York, where discussion centred on SWIFT's strategic priorities and services updates.

### Innotribe

In 2017 Innotribe continued its mission to showcase innovation and new thinking from around the industry, and to connect FinTechs and startups with financial institutions to foster the creation of cutting-edge new products. The team ran a number of challenge events, including an Industry Challenge in Singapore, focused on bringing new value to SWIFT's global payments innovation (gpi) platform. Innotribe will continue to work with the winners to help realise the most promising proposals through 'proof of value' exercises.

### SWIFT Institute

In 2017 the SWIFT Institute celebrated its fifth year. Five new research grants were issued, covering diverse topics including financial crime, new technology, market infrastructures and the future of transaction banking. Five new research papers were published, covering cyber security, open APIs and regulatory impact on innovation.

The institute ran several events, including two cyber security conferences (London and Singapore), a full programme at Sibos, and contributed speakers and topics to SWIFT Business Forum events in London, Athens and Toronto.

The 2017 Student Challenge was held in Canada on the topic 'How can bank channels be secured against ever-increasing cyber attacks?'. The winning team, 'Team Pulse OS' from the University of Toronto, was announced at the closing plenary of Sibos, and awarded a prize of CAD20,000. The 2018 Student Challenge will be held in Australia, looking at how to keep information private in an open banking environment. The winner will be chosen and announced at Sibos Sydney.

### Standards

In 2017 the Standards team ran Standards Forum events in London, New York, Zurich, Kiev and Moscow, culminating in a four-day programme of presentations, panel sessions and workshops at Sibos in Toronto. The stand-out themes were: standards and regulation, with a particular focus on payments data quality, and the application of standards to new technology, including DLT and API. These topics were further developed in information papers later published on swift.com.

Standards also continued its initiative to harmonise use of ISO 20022 amongst Market Infrastructures (MIs). Two MI Summit events were held, in London and Toronto, bringing together major Market Infrastructures to network and learn from one another, and to share developments in standards harmonisation, including progress towards common market practice for high-value payments systems, and a new information paper on ISO 20022 adoption strategies.

The MyStandards product portfolio continues to evolve, with the announcement at Sibos of a significant new capability, SWIFT Translator, a format translation offering that integrates with MyStandards to provide an end-to-end solution for standards implementation, from specification to run-time deployment.

At the September 2017 meeting of the SWIFT Board, Standards announced a study to explore migration of cross-border MT traffic to ISO 20022. A consultation with all relevant stakeholders is planned for the first half of 2018.

### Sibos

Sibos 2017 took place in Toronto, and was attended by 8,062 delegates from 149 countries, making it the largest Sibos ever held in the Americas. A total of 187 exhibitors presented financial products, IT solutions and services. Under the theme of 'Building for the Future', more than 250 conference sessions explored the industry's most topical issues, including cyber security, Artificial Intelligence, the impact of geopolitical and regulatory shifts, and data and identity. The conference programme featured more than 400 speakers, including icons of industry such as Satya Nadella, CEO of Microsoft, and Sir Tim Berners-Lee, inventor of the World Wide Web.

# SWIFT2020

## Grow the core

## Build the future

**Published in 2015, the strategy is designed to respond effectively to external challenges and drivers of change, by building on previous successes and taking a 'grow the core, build the future approach'.**

In the second full year of the strategy's execution, our activities to strengthen the core have focused on expanding our Market Infrastructure (MI) offering and building up our financial crime compliance products and services. *SWIFT2020* is at the forefront of our efforts to help our community fight cyber crime, manage regulatory compliance, and to adapt to increasing demands for faster and more efficient payments.

**Grow and strengthen core messaging services for payments and securities**
In line with our core mission to provide secure and reliable messaging services, we made progress on a number of our strategic growth initiatives.

In 2017, we strengthened the SWIFT platform by:

- Expanding our interface and connectivity solutions to enhance customer experience, through further adoption of the Alliance Messaging Hub, allowing customers to connect to multiple networks around the world, including integration with back-office systems, to allow seamless routing of financial messages.
- Introducing new technologies to enable new services around instant messaging.
- Launching SWIFTNet, Alliance Gateway Instant and AMH Instant to support growing demands.
- Rolling out our global payments innovation (gpi) Connector, part of the Alliance Integration platform.
- Successfully introduced our Post-trade Risk Alerting Service (PtRA), which helps to reduce operational risk in trade settlement.
- We also strengthened our solution in the FX space, with FX Performance Insights, providing customisable, ready-to-consume reporting.
- Our CSD Community Offering, launched in 2016, gained traction across all regions in 2017 with Austria, Argentina and Hungary being the first to sign, giving their respective communities the best choice in terms of channel, standards and pricing.

**Expand and deepen offerings for Market Infrastructures**
We continued to invest in structural and regional initiatives affecting securities and payment MIs. In November 2017, we successfully delivered the Australian New Payments Platform (AU-NPP) – a new infrastructure for instant payments. In Europe, we are using many elements of this system to enable seamless connectivity to regional clearing and settlement mechanisms (CSMs). We provided our Alliance Messaging Hub (AMH) solution to a major clearing organisation in the US, and worked closely with the Canadian community as they modernise their payments infrastructure.

As the European Central Bank's TARGET2-Securities (T2S) platform is gearing up to provide a single settlement environment for the Euro area, we continued to support the market and our community through our second-generation MI technology solutions.

**Enabling growth**
In an evolving financial market, shaped by an uncertain economic and political environment, we continue to offer the global SWIFT community stability, resilience and operational excellence. *SWIFT2020* anchors our strategic investments against this shifting backdrop and we focused on three priority areas:

- global payments innovation (gpi) – cross-border payments, transformed
- Financial crime compliance (FCC) – meeting the growing compliance challenge
- the Customer Security Programme (CSP) – reinforcing the security of the global financial community

Throughout the year, we continued to take a leading role in standards by pursuing the implementation of ISO 20022 by market infrastructures (MIs). We also complemented our consultancy, standards management and translation services with the introduction of SWIFT Translator, a message translation tool that helps users define, map and validate messages from any format to ISO 20022 or MT.

In 2017 we increasingly looked to standardisation to support the introduction of Distributed Ledger Technology (DLT), Artificial Intelligence (AI) and emerging new technologies, whilst progressing our analytics and services support. SWIFT is taking a leading role in creating open business standards for DLT, building on our extensive experience and relationships with industry players, regulators and standards bodies. This will help achieve a consistent and harmonised approach from the outset, paving the way for success.

**Global payments innovation (gpi) – cross-border payments, transformed**
In 2017 we continued to promote gpi's adoption as the standard in correspondent banking, exploring the potential of open APIs to enhance both our services and corporate customer experience.

**Build our financial crime compliance portfolio**
Customers in almost every country in the world now use SWIFT's financial crime compliance (FCC) services. Our FCC suite continues to be a key priority and we are building on our portfolio to meet evolving industry needs, with an increasing focus on sanctions, analytics and fraud prevention solutions. By leveraging industry-defined standards, a common infrastructure and shared costs, in close collaboration with our customers, we made significant inroads into our financial crime compliance growth strategy.

**Customer Security Programme (CSP) – reinforcing the security of the global financial community**
In April 2017 we rolled out the Customer Security Controls Framework as part of our Customer Security Programme. SWIFT customers were required to attest their level of compliance against a set of 27 security controls by the end of 2017. By year end, 89% of all SWIFT customers attested their level of compliance. Combined, these institutions account for over 99% of all FIN messages sent over the SWIFT network.

***SWIFT2020* – Strategic priorities**

## Corporate Social Responsibility

# Operating responsibly and sustainably

# Engaging with our communities

# Facilitating business sustainability

**21%**
of SWIFT staff engaged in CSR activities

**35%**
of new hires are female

**40**
countries in which SWIFT is active in CSR programmes and initiatives

**132,000km**
commuted to work by bicycle in Belgium and the Netherlands

**1,000,000km**
driven by employees emitting zero $CO_2$ emissions since 2015

**In 2017 SWIFT progressed on its three CSR priorities: (1) operating responsibly and sustainably; (2) caring for our communities; and (3) facilitating business sustainability. Our CSR efforts are aligned with the United Nations Global Compact (UNGC), to which we have adhered to since 2012 and continue to support. We also contributed to the Sustainable Development Goals (SDG) adopted in September 2015 by the UN General Assembly.**

**Operating responsibly and sustainably**
SWIFT has reduced the impact of its activities on the environment. In 2017, we reviewed the methodology to establish our climate footprint, taking into account newest insights and methodologies defined by the international community following the 2015 Paris Agreement on climate change. We use renewable energy whenever feasible and, since 2012, we have compensated emissions caused by work-related travel and events.

**Energy efficiency**
In 2017 SWIFT extended its hot-desking programme to more SWIFT offices and data centres, allowing us to further rationalise office space and control electricity consumption while staff continues to grow. Significant contributions were also achieved by installing energy-efficient windows and frames in one of our buildings. Following a long-term renewal plan, SWIFT also replaced air handling units by energy efficient models in an operating centre and optimised the related controls to further reduce the energy consumption. In our headquarters, we fine-tuned the newly installed Building Management System, replaced old lamp bulbs with LED-lighting, and carried out an energy efficiency audit to highlight additional potential savings. SWIFT's electricity in Belgium, Switzerland, the Netherlands and the United Kingdom originates from renewable sources, and partially in Spain. During 2017, we renewed our electricity contract in the Netherlands, ensuring the sourcing of renewable energy for the coming three years. We continue to investigate renewable energy suppliers in other countries.

**Mobility**
Our company car fleet in Belgium and the Netherlands included 30 electric and 85 hybrid plug-in cars by the end of 2017. As a result, employees have driven over 1 million kilometres emitting zero $CO_2$ emissions since the programme was launched in 2015. For the fourth year running, SWIFT was awarded the 5-star label from Tous Vélos-Actifs, in recognition of our proactive and innovative policy to promote alternative mobility and commuting by bicycle. At our headquarters in Belgium alone, SWIFT staff covered 105,463 km by cycling to work in 2017 and in the Netherlands they reached close to 27,000 km.

**Sibos**
At Sibos in Toronto, SWIFT implemented a number of green measures regarding waste, water consumption, biodiversity and recycling. The EcoCab service available in Toronto enabled emission-free commuting and, upon registration, delegates were able to contribute to reforestation projects through WeForest, an international NGO thriving to advance innovative, scalable and lasting solutions to restore forest landscapes across the world.

**Diversity and inclusion**
We organised a number of events to promote and create awareness of female empowerment. We developed our initiative, Balance@SWIFT, through which staff can discuss diversity and inclusion issues. We achieved our target of 35% of new hires being female. We launched the Global Ambassadors Programme, which enables staff worldwide to organise and carry out events around diversity and inclusion with local relevance. In August, our CEO signed the UN Woman Empowerment Principles, expressing our support for advancing equality between women and men. Diversity and inclusion was again an important feature of the Sibos conference programme.

**Staff engagement in our communities**
In 2017, through our various programmes and initiatives, we were active in more than 40 countries on five continents.

The involvement of our employees in CSR initiatives remains the cornerstone of our programme. Over 21% of staff were involved in one or more CSR activities during the past year. Staff were active in organising onsite sales; donating blood; participating in Team with Spirit events such as fundraising, cycling, swimming, running, climbing mountains, tutoring refugee children, cleaning beaches, singing for charities, and donating food baskets and toys at Christmas.

As in previous years, SWIFT matched staff donations through fundraising campaigns for United Way and the American Cancer Society. SWIFT also continued to support our long-lasting partner United Fund for Belgium, a non-profit organisation hosted on SWIFT premises that redistributes 100% of its donations to small charities involved in child welfare, poverty reduction, support for handicapped persons and social integration and training.

Following the hurricanes that hit the Americas in 2017, SWIFT made donations to the Red Cross and to a school in Barbuda, one of the most affected islands in the Caribbean. Additionally, staff shipped boxes filled with goods to victims in Puerto Rico and following the Mexican earthquake Sibos delegates donated to Save the Children Mexico. On top of this, SWIFT contributed to the emergency funds of Doctors without Borders.

**Children and education**
Through our staff engagement, we provided support for children in need across the world, financing education for orphans, uneducated girls, children with a long-term or terminal illness, disabled and autistic children, victims of war, refugees, homeless children or those living on the streets and unprivileged children from migrant families.

SWIFT helped local charities supporting people in the regions in which we host conferences and business forums. These included the Children's Society in Singapore; Pestalozzi Kinderdorf in Switzerland; Cliniclowns in the Netherlands; Face for Children in Need in Egypt; ECPAT in Sweden; Breakthrough in the US; and SOS Children's Villages in China, France, Greece, Poland, Romania, Ivory Coast, India, Mexico, Russia, Romania, Spain and Tanzania. At Sibos Toronto we donated to Sketch, an arts platform for poverty-stricken young people.

These initiatives support the achievement of the UN Sustainable Development Goal 4, which aims to ensure inclusive and equitable quality education and promote lifelong learning opportunities for all.

**Facilitating business sustainability**
To reinforce our links with local communities, SWIFT develops and promotes partnerships with organisations engaged in financial inclusion and education in emerging countries. On top of the Mann Deshi Foundation in India, Nairobits Trust in Kenya and Phakamani Foundation in South Africa, we strengthened our support of our two global key partners, Teach for All and Fundación Capital.

Teach for All works to ensure that the academic success of a child no longer depends on his or her socio-economic background. Young local university graduates are recruited and coached to teach children in socio-economically underprivileged schools. Through specific partnerships in Argentina, Bangladesh, Columbia, Ghana and Nigeria, we support thousands of children on a global scale.

Financial education and inclusion are important to SWIFT. Fundación Capital is a pioneer in inclusive finance and a testing ground for innovation in asset-building, working to eliminate poverty by expanding access to capital, information, training, and productive opportunities. SWIFT has supported Fundación Capital by helping to finance the development of tablet-based applications aimed at providing financial education to youth and women in Brazil, Mexico, Peru, Tanzania and Vietnam. Fundación Capital received the Schwab Foundation's Social Entrepreneur of the Year 2017 award. This contributes to the UN Sustainable Development Goal 1, which is aimed at ending poverty.

For more information on SWIFT CSR activities, please consult our UNGC Communication on Progress: www.unglobalcompact.org

# Messaging facts and figures

## FIN

**Financial institutions use FIN for individual, richly featured messaging which requires the highest levels of security and resilience. Features include validation to ensure messages conform to SWIFT message standards, delivery monitoring and prioritisation, message storage and retrieval.**

In 2017 more than 7.1 billion FIN messages, or an average of 28.1 million messages per day, were sent over SWIFT. This is an increase in total FIN volume of 8.4 percent over 2016.

SWIFT recorded three FIN peak days in 2017. The latest one was on 30 November when close to 33 million messages went over the SWIFT network. This peak was the result of the strong growth recorded over the last months, combined with month-end reporting.

### FIN share by market

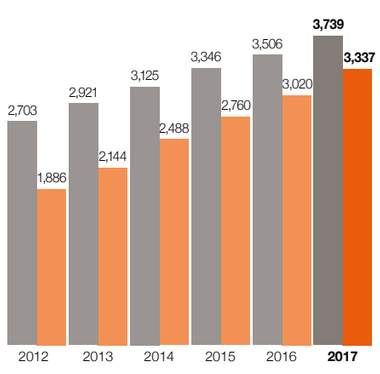
2017 volume (millions)

| | |
|---|---|
| Payments[1] | 3,485 |
| Securities | 3,232 |
| Treasury | 305 |
| Trade | 36 |
| System | 18 |

[1] including FIN Copy messages

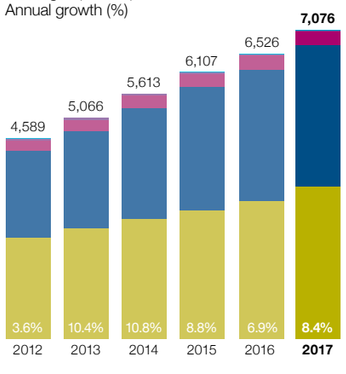
### Reporting messages versus non-reporting messages

Messages (millions)




### FIN traffic evolution

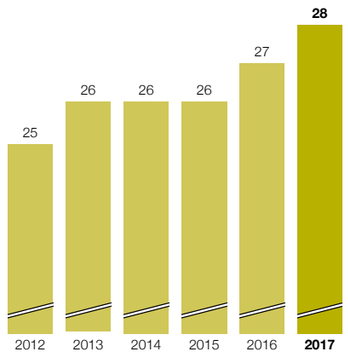
Messages (millions)
Annual growth (%)




### Payment messages

Payments volume recorded a strong increase (11.0%) compared to historical trends. This solid performance reflects positive economic conditions and outlook, and was further fuelled by traffic gains. Growth was almost equally driven by reporting and non-reporting messages. As usual, the highest month volume-wise was December, with Payments volumes reaching an average of 15.7 million messages/day.

### Low value payment (LVP) systems connected to SWIFT




### Reporting messages

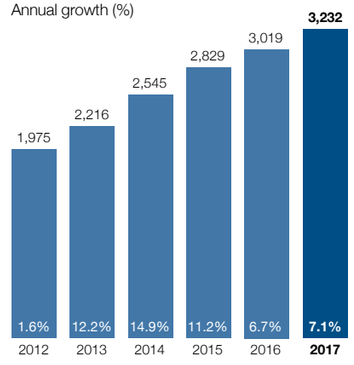
Reporting messages grew by 10.5 percent during the year, outperforming the non-reporting messages growth of 6.6 percent. Thus, reporting messages drove close to 60% of the SWIFT total volume growth, in particular in the Securities area. Over the last five years, the weight of the reporting messages in the total FIN traffic has increased from 41 percent in 2012, to 47 percent in 2017.

### Securities messages

Securities traffic grew by 7.1%, despite FIN traffic migrating to TARGET2-Securities. The impact of traffic migrated to TARGET2-Securities was lower than expected and some large securities players showed double-digit growth. Reporting flows accounted for two-thirds of the growth.

### FIN Securities traffic evolution

Messages (millions)
Annual growth (%)

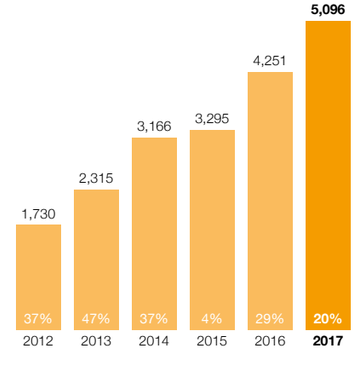



## FileAct

**FileAct is an advanced, secured and resilient file transfer protocol tailored to the need of customers to exchange freely formatted transactions in bulk mode. It is primarily used to exchange large batches of low-value payments and the corresponding reporting.**

At 20%, FileAct traffic growth recorded strong double-digit growth in 2017. TARGET2-Securities contributed to this solid performance. Low-value payments remained the largest FileAct volume contributor, and have grown thanks to gains in the European cards clearing business and new Market Infrastructures starting to use SWIFT. The Corporates segment showed another year of steady growth.

| | |
|---|---|
| FileAct volume in billions of characters | 5,096 |
| FileAct volume in millions of files | 153 |
| Live and pilot users | 2,935 |
| Services using FileAct | 177 |




[2] growth rate 2013 is based on adjusted 2012 volumes taking into account the increase file compression rate. The compression rate changed due to customer migration to a new version of SWIFTNet Link (SNL) which applies compression automatically

## InterAct

**InterAct is a versatile protocol that supports different types of usage and business. It is primarily used by market infrastructures to support ISO 20022 messaging. Our Store & Forward version of InterAct has been enriched to provide the same level of functionalities as FIN.**

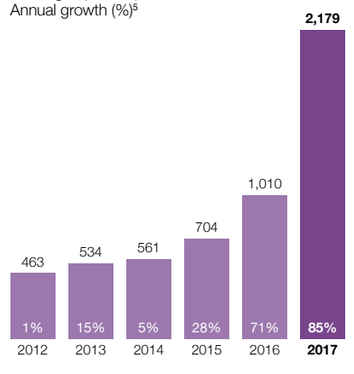
TARGET2-Securities was the key driver for the InterAct traffic growth in 2017, as the official migration plan was being completed, with the final wave mid-September 2017. Over the full year, TARGET2-Securities InterAct traffic represented over 65% of total InterAct traffic.

| | |
|---|---|
| InterAct messages[3] | 2,179 million |
| Live and pilot users[4] | 2,288 |
| Services using InterAct[3] | 69 |

[3] including CREST
[4] including CREST, excluding RMA

### InterAct traffic evolution

Messages (millions)
Annual growth (%)[5]




[5] growth rates 2015–2017 are based on adjusted historical volumes, neutralising the impact of the CLS platform migration

All figures and percentages have been calculated using unrounded figures. Totals may not add up due to rounding.

# Board and Executive

## SWIFT Board

**Yawar Shah**
Chairman of the Board of Directors, SWIFT
Managing Director, Citigroup, United States
SWIFT Director since 1995
Chairman of the Franchise Risk Committee of the Board, SWIFT

**Stephan Zimmermann**
Deputy Chairman of the Board of Directors, SWIFT
Divisional Vice Chairman, Wealth Management, UBS AG, Switzerland
SWIFT Director since 1998
Chairman of Human Resources Committee of the Board, SWIFT

**Eddie Astanin**
Chairman of the Executive Board of NSD, Russia
SWIFT Director since 2015

**Gianfranco Bisagni**
Co-Head of Corporate and Investment Banking (CIB), Unicredit, Italy
SWIFT Director since 2017

**Mark Buitenhek**
Global Head of Transaction Services, ING, The Netherlands
SWIFT Director since 2012
Chairman of the Banking & Payments Committee of the Board, SWIFT

**Fabrice Denèle**
Senior Vice President, Partnerships & Interbank Relationships and Head of Consumer Solutions, Natixis Payment Solutions, France
SWIFT Director since 2009

**John Ellington**
Director, Shared Services, Services, RBS, United Kingdom
SWIFT Director since 2005
Chairman of the Technology & Production Committee of the Board, SWIFT

**Göran Fors**
Deputy Head of Investor Services, SEB, Sweden
SWIFT Director since 2009
Chairman of the SWIFT Securities Committee of the Board, SWIFT

**Mark Gem**
Member of the Executive Board, Clearstream International S.A., Luxembourg
SWIFT Director since 2013

**Rob Green**
Head of Payments Market Infrastructure, Banking Group Treasury, FirstRand, South Africa
SWIFT Director since 2009
Chairman of the Audit & Finance Committee, SWIFT

**Frederic Hannequart**
Chairman, Euroclear Bank, Chief Business Officer, Euroclear Group, Belgium
SWIFT Director since 2014

**Søren Haugaard**
Global Head of Trade and Supply Chain Finance, Danske Bank, Denmark
SWIFT Director since 2015
Chair of the SWIFT Corporate Advisory Group (CAG).

**Jose Luís Calderón Igareda**
Managing Director, Global Head of GTB, Santander Global Corporate Banking (GCB), Member of GCB Executive Committee, Santander, Spain
SWIFT Director since 2017

**Lisa Lansdowne-Higgins**
Vice President, Business Deposits and Treasury Solutions, RBC, Canada
SWIFT Director since 2013

**Emma Loftus**
Managing Director, Global Payments and FX Product Executive, J.P. Morgan Treasury Services, USA
SWIFT Director since 2016

**Stephen Lomas**
Managing Director, Head of Market Policy, Global Transaction Banking, Deutsche Bank, Germany
SWIFT Director since 2013

**Lynn Mathews**
Chairman of the Australian National Member Group, Australia
SWIFT Director since 1998

**Stephan Müller**
Divisional Board Member and Group CIO, Commerzbank, Germany
SWIFT Director since 2015

**Hiroshi Nakatake**
General Manager, Transaction Banking Division, The Bank of Tokyo-Mitsubishi UFJ, Japan
SWIFT Director since 2017

**Bock Cheng Neo**
Executive Vice President, Head of Global Transaction Banking, OCBC Bank, Singapore
SWIFT Director since 2015

**Alain Pochet**
Head of Clearing, Custody and Corporate Trust Services, BNP Paribas Securities Services, France
SWIFT Director since 2010

**Russell Saunders**
Managing Director, Global Payments, Lloyds Banking Group, United Kingdom
SWIFT Director since 2016

**Ulrich Stritzke**
Managing Director, Credit Suisse, Switzerland
SWIFT Director since 2012

**Patrick Tans**
Senior General Manager, Banking Products, KBC Bank, Belgium
SWIFT Director since 2015

**Jianguang Wu**
General Manager, Bank of China, Head Office Clearing Department, China
SWIFT Director since 2017

During the course of 2017, the following Directors left the Board:
Claudio Camozzo, UniCredit, Italy
Kyoichi Nagata, The Bank of Tokyo-Mitsubishi UFJ, Japan
Javier Santamaria, Banco Santander, Spain
Qingsong Zhang, Bank of China, Head Office Clearing Department, China

## Our executive team

**Gottfried Leibbrandt**
Chief Executive Officer

Gottfried Leibbrandt was appointed Chief Executive Officer of SWIFT in July 2012. He joined SWIFT in 2005 to focus on the development of the *SWIFT2010* strategy. Upon completion of the strategy, he was appointed Head of Standards, and then in 2007 he was promoted to Head of Marketing. Leibbrandt was a key architect behind the *SWIFT2015* strategy.
Prior to joining SWIFT, Leibbrandt worked at McKinsey & Company for 18 years as a partner in the Amsterdam office and a co-leader of the European payments practice.

**Marcel Bronmans**
Chief Operations Officer

Marcel Bronmans was appointed as Chief Operations Officer in February 2015. He joined SWIFT in 1987 and has held a variety of management positions in the IT and Operations area at SWIFT, including that of Director of Technology Operations. Most recently, Bronmans held positions as Chief Risk Officer and Head of Human Resources.

**Stephen Gilderdale**
Chief Platform Officer

Stephen Gilderdale was appointed Chief Platform Officer in October 2017. He was previously Managing Director for the UK, Ireland and Nordics, with responsibility for strategic client relationship management and business development. Gilderdale has over 20 years' experience across a number of operations, technology and business development roles, and prior to joining SWIFT in 2007, held senior management positions at Accenture where he worked across a variety of financial institutions, including securities marketplaces, banks and card operators.

**Luc Meurant**
Chief Marketing Officer

Luc Meurant was appointed as Chief Marketing Officer in October 2017. He was previously head of the Financial Crime Compliance Services division at SWIFT. Meurant joined SWIFT in 2002 from McKinsey & Company, where he specialised in serving financial institutions, payments systems and telecommunications firms. Earlier in his career he worked at Euroclear, where he specialised in securities transactions across European markets.

**Javier Pérez-Tasso**
Chief Executive, Americas & UK Region

Javier Pérez-Tasso is Chief Executive Americas, UK, Ireland and Nordics at SWIFT. Appointed in September 2015, he is responsible for key client relationships and business development across the region. Previously, Pérez-Tasso served as Chief Marketing Officer, whilst earlier in his career he held several senior leadership positions in SWIFT's sales and marketing divisions.

**Alain Raes**
Chief Executive, EMEA and Asia Pacific

Alain Raes was appointed Chief Executive of the EMEA Region in September 2007 and added the role of Chief Executive Asia Pacific in January 2013. He was previously Director of the Continental Europe region, having joined SWIFT in 1990. Prior to joining SWIFT he worked at Citibank, Belgium and Fortis Bank, Singapore.

**Francis Vanbever**
Chief Financial Officer

Francis Vanbever was appointed to his current position in 1997. Vanbever joined SWIFT in 1988. Prior to SWIFT he held various financial responsibilities for the Belgian and European operations of Exxon Chemicals.

**Craig Young**
Chief Information Officer

Craig Young was appointed Chief Information Officer in February 2015. He joined SWIFT from Verizon Communications, where he had worked for 20 years, most recently as Senior Vice President and Chief Information Officer.

The General Counsel, the Chief Risk Officer and the Chief Auditor report directly to the CEO, and the Head of Human Resources reports to the CFO. The CEO represents the General Counsel, the Chief Risk Officer and the Chief Auditor on the Executive Committee, whilst the CFO represents the Head of Human Resources.

Patrick Krekels, General Counsel and Board Secretary
Dina Quraishi, Chief Risk Officer
Peter De Koninck, Chief Auditor

# SWIFT Governance

**SWIFT is a cooperative company under Belgian law and is owned and controlled by its shareholders. SWIFT shareholders elect a Board composed of 25 independent Directors which governs the Company and oversees management. The Executive Committee is a group of full-time employees led by the Chief Executive Officer.**

**Board Director nominations**
SWIFT's Board composition is designed to reflect usage of SWIFT messaging services, ensure SWIFT's global relevance, support its international reach and uphold its strict neutrality.

Each nation's usage of SWIFT's messaging services determines both SWIFT shareholding allocations and the number of Board Directors that each nation is entitled to.

SWIFT shareholdings are determined by a set formula, and the nomination process and the composition of the Board follow rules set out in SWIFT's by-laws. Shares are reallocated based on the financial contribution of shareholders for network-based services. This ensures that the composition of the Board reflects SWIFT's shareholders around the world. Depending on a nation's shareholder ranking, it may propose one or two Directors to the Board or join other nations to collectively propose a Director:

a. For each of the first six nations ranked by number of shares, the shareholders of each nation may collectively propose two Directors for election. The number of Directors proposed in this way must not exceed 12.

b. For each of the ten following nations ranked by number of shares, the shareholders of each nation may collectively propose one Director for election. The number of Directors proposed in this way must not exceed ten.

c. The shareholders of those nations which do not qualify under 'a. or b.' above may join the shareholders of one or more other nations to propose a Director for election. The number of Directors proposed in this way must not exceed three.

The total number of Directors cannot exceed 25.

**Director elections**
Once the proposed Director nominees have been vetted, they are elected as Board Directors by SWIFT shareholders at the Annual General Meeting for a renewable three-year term. Every year the Board elects a Chairman and a Deputy Chairman from among its members. It meets at least four times a year.

**Director remuneration**
Members of the Board do not receive any remuneration from SWIFT. They are reimbursed for the travel costs incurred in the performance of their mandate. SWIFT reimburses the employer of the Chairman of the Board for the share of the Chairman's payroll and related costs that represent the portion of the time dedicated to SWIFT.

**Board committees**
The Board has six committees.
The committees provide strategic guidance to the Board and the Executive Committee and review progress on projects in their respective areas.

- The Audit and Finance Committee (AFC) is the oversight body for the audit process of SWIFT's operations and related internal controls. It commits to applying best practice for Audit Committees to ensure best governance and oversight in the following areas:
  - Accounting, financial reporting and control
  - Legal and regulatory oversight
  - Security
  - Budget, finance and financial long-term planning
  - Ethics programmes
  - Risk management (in cooperation with the Franchise Risk Committee (FRC))
  - Audit oversight

  The AFC meets at least four times per year with the CEO, CFO, CRO, General Counsel and the Chief Auditor, or their pre-approved delegates.

  The AFC may request the presence of any member of SWIFT staff at its discretion. External auditors are present when their annual statements/opinions are discussed and whenever the AFC deems appropriate.
- The Franchise Risk Committee (FRC) assists the Board in its oversight of the Company's management of key risks, including strategic and operational risks, as well as the guidelines, policies and processes for monitoring and mitigating such risks. The FRC's role includes oversight of risk management of SWIFT. The FRC coordinates with the Chairs of the AFC and TPC, and focuses on risks not covered by those committees. The FRC is chaired by the Chairman of the Board, and includes the Vice-Chairman, the Chairs of the AFC and TPC, as well as two other Board members. The Committee meets at least three times a year, out of the normal Board cycle.
- The Human Resources Committee (HRC) oversees executive compensation. It assesses the Company's performance and decides on the remuneration packages for members of the Executive Committee and other key executives. It monitors employee compensation and benefits programmes, including the provisioning and funding of the pension plans. It also approves appointments to the Executive Committee and assists in the development of the organisation, including succession planning. The Board Chairman and Deputy Chairman are routinely members of the HRC, which meets at least four times per year with the CEO, the Head of Human Resources and the CFO on financial and performance measures. The HRC has delegated powers from the Board in these matters. The HRC also meets without SWIFT executives several times a year.
- The Banking & Payments Committee (BPC) and the SWIFT Securities Committee (SSC) focus on segment-specific developments.
- The Technology & Production Committee (TPC) covers technology and production developments.

**Audit process**
SWIFT's Chief Auditor has a dual reporting line: a direct functional reporting line to the Chair of the AFC and also a direct administrative reporting line to the CEO. Given the sensitivity of external auditors performing consultancy work for management, the AFC annually reviews spending and trends related to external audit firms. To ensure objectivity, the mandates of the external auditors, as well as their remuneration, are approved by the AFC.

**Two mandates for external audit**
- Ernst & Young, Brussels has held the Financial Audit mandate since June 2000. Their mandate was renewed in June 2015 and runs to June 2018. Their financial Audit Report can be found in the 2017 Consolidated Financial Statements.
- PwC, London has held the Security Audit mandate since September 2003. In 2016 their mandate for third-party assurance reporting (ISAE 3000) was renewed for three years, to end in 2019. For the 2017 calendar year, SWIFT is providing standalone ISAE 3000 Type 2 reports for SWIFTNet and FIN, T2S and Alliance Lite2. Each report includes PwC's opinion on the design adequacy and operating effectiveness of the control activities that help achieve the control objectives in the areas of risk management, security management, technology management, resilience and user communication (in line with CMPIIOSCO's Expectations for Critical Service Providers). ISAE 3000 is an international standard enabling service providers, such as SWIFT, to give independent assurance on their processes and controls to their customers and their auditors. The ISAE 3000 reports for SWIFTNet and FIN and Alliance Lite2 are made available to shareholding institutions or registered SWIFT users on request by email to ISAE_3000@swift.com. The ISAE 3000 report for T2S is restricted to the Eurosystem and T2S Directly Connected Actors.

**Oversight**
SWIFT maintains an open and constructive dialogue with its oversight authorities. SWIFT is overseen because of its importance to the smooth functioning of the worldwide financial system, in its role as provider of messaging services. SWIFT is overseen by the central banks of the G-10 countries. Under an arrangement with the G-10 central banks, the National Bank of Belgium, the central bank of the country in which SWIFT's headquarters is located, acts as lead overseer. In 2012 this framework was reviewed and a SWIFT Oversight Forum was established, through which information sharing on SWIFT oversight activities was expanded to a larger group of central banks. The issues to be discussed may include the five High Level Expectations that relate to risk identification and management, information security, reliability and resilience, technology planning, and communication with users.

**User representation**
SWIFT's National Member Groups and National User Groups help to provide a coherent global focus by ensuring a timely and accurate two-way flow of information between SWIFT and its users.

The National Member Groups comprise all SWIFT shareholders from a nation, and propose candidates for election to the SWIFT Board of Directors. They act in a consultative capacity to the Board and management, and serve the interests of their nation's shareholders by coordinating their views. Each National Member Group is chaired by a representative who is elected by the SWIFT shareholders of that nation.

National User Groups comprise all SWIFT users from a nation and act as a forum for planning and coordinating operational activities. Each National User Group is chaired by a representative who is a prime line of communication between the national user community and SWIFT.

# Oversight

## International cooperative oversight

## Effective controls and processes

## Open and constructive dialogue

## Reviewing operational risk

**The oversight objectives centre on: risk identification and management, information security, reliability and resilience, technology planning, and communication with users.**

Central banks have the explicit objective of fostering financial stability and promoting the soundness of payment and settlement systems.

While SWIFT is neither a payment nor a settlement system, and is therefore not regulated as such by central banks or bank supervisors, it is subject to central bank oversight as a critical service provider. A large and growing number of systemically important payment systems have become dependent on SWIFT, which has thereby acquired a systemic character. As a result, the central banks of the G-10 countries agreed that SWIFT should be subject to cooperative oversight by central banks. SWIFT has been subject to oversight since 1998.

The arrangement was last reviewed in 2012 when the SWIFT Oversight Forum was set up. Information sharing on SWIFT oversight activities was thereby expanded to a larger group of central banks.

**An open and constructive dialogue**
SWIFT is committed to an open and constructive dialogue with its oversight authorities. The National Bank of Belgium (NBB) acts as the lead overseer, and is supported by the G-10 central banks. The oversight primarily focuses on ensuring that SWIFT has effective controls and processes to avoid posing a risk to the financial stability and the soundness of financial infrastructures.

The NBB is lead overseer, as SWIFT is incorporated in Belgium. Other central banks also have a legitimate interest in, or responsibility for, the oversight of SWIFT, given SWIFT's role in their domestic systems.

As is generally the case for payment systems oversight, the main instrument for oversight of SWIFT is moral suasion. Overseers place great importance on the constructive and open dialogue that is conducted on the basis of mutual trust with the SWIFT Board and senior management. Through this dialogue, overseers formulate their recommendations to SWIFT.

A protocol signed between the NBB and SWIFT lays down the common understanding of overseers and SWIFT. The protocol covers the oversight objectives and the activities that are undertaken to achieve those objectives. The protocol is revised periodically to reflect evolving oversight arrangements.

**Objectives, areas of interest and limitations**
In their review, overseers seek assurances that SWIFT has put in place appropriate governance arrangements, structures, processes, risk management procedures and controls that enable it to effectively manage potential risks to financial stability and to the soundness of financial infrastructures, to the extent that they are under SWIFT's control.

In 2007 the overseers developed specific oversight expectations applicable to SWIFT, known as the 'High Level Expectations for the oversight of SWIFT' (HLEs). The High Level Expectations document the five categories of expectations that overseers have vis-à-vis the services SWIFT provides to the global financial infrastructure. The five expectations relate to: risk identification and management, information security, reliability and resilience, technology planning, and communication with users.

Overseers review SWIFT's identification and mitigation of operational risks, including cyber security, and may also review legal risks, transparency of arrangements and customer access policies. The overseers may also discuss SWIFT's strategic direction with the SWIFT Board and senior management.

This list of oversight fields is indicative, not exhaustive. Overseers will undertake those activities that provide them comfort that SWIFT is paying proper attention to the objectives described above. Nevertheless, SWIFT continues to bear the responsibility for the security and reliability of its systems, products and services. The oversight of SWIFT does not grant SWIFT any certification, approval or authorisation.

**International cooperative oversight**
As lead overseer, the NBB conducts the oversight of SWIFT together with the G-10 central banks: Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d'Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank, Swiss National Bank, Bank of England and the Federal Reserve System (USA), represented by the Federal Reserve Bank of New York and the Board of Governors of the Federal Reserve System.

In the SWIFT Oversight Forum, these central banks are joined by other central banks from major economies: Reserve Bank of Australia, People's Bank of China, Hong Kong Monetary Authority, Reserve Bank of India, Bank of Korea, Central Bank of Russia, Saudi Arabian Monetary Agency, Monetary Authority of Singapore, South African Reserve Bank and the Central Bank of the Republic of Turkey. The SWIFT Oversight Forum provides a forum for the G-10 central banks to share information on SWIFT oversight activities with a wider group of central banks.

**Oversight structure — oversight meetings**
The NBB monitors SWIFT on an ongoing basis. It identifies issues relevant to SWIFT oversight through the analysis of documents provided by SWIFT and through discussions with SWIFT management. The NBB maintains a close relationship with SWIFT, with regular ad hoc meetings, and serves as the central banks' entry point for the cooperative oversight of SWIFT. In this capacity, the NBB chairs the senior policy and technical groups that facilitate the cooperative oversight, provides the secretariat and monitors the follow-up of any decisions taken.

**Access to information**
In order to achieve their oversight objectives, the overseers need timely access to all information that they consider relevant. Typical sources of information are SWIFT Board papers, security audit reports, incident reports and incident review reports. Presentations by SWIFT staff and management represent another important source of information for the overseers.

Finally, SWIFT assists the overseers in identifying internal SWIFT documents that might be relevant to address specific oversight questions. Provisions on the confidential treatment of non-public information are included both in the protocol between the NBB and SWIFT, and in the bilateral Memoranda of Understanding between the NBB and each of the other cooperating central banks. The official description of the NBB's oversight role can be found in the Financial Market Infrastructures and Payment Services Report published by the National Bank of Belgium and is available on its website www.nbb.be.

# Security audit and financial performance

**2017 Security audit statement**
The Directors and management acknowledge their responsibility for maintaining an effective system of internal control. Management is satisfied that, for the period 1 January 2017 to 31 December 2017, the control policies and procedures were operating with sufficient effectiveness to ensure that the control objectives with regard to risk identification and management, information security, reliability and resilience, technology planning and communication with users were met. The control objectives were specified by SWIFT management, in line with the overseers' High Level Expectations for SWIFT and CMPI-IOSCO's Expectations for Critical Service Providers.

PwC were retained by the Directors to review the adequacy of design and the operating effectiveness of the manual and computer-based controls and the control policies for the FIN and SWIFTNet messaging services, Alliance Lite2 and T2S specified by SWIFT management covering the period from 1 January to 31 December 2017.

Their examination was made in accordance with the International Standard for Assurance Engagements (ISAE) 3000, established by the International Auditing and Assurance Standards Board (IAASB). ISAE 3000 is an international standard enabling service providers, such as SWIFT, to give independent assurance on their processes and controls to their customers and their auditors. The ISAE 3000 report provides information and assurance on the security and reliability of SWIFT's main messaging services, Alliance Lite2 and T2S.

## Key figures

For the year ended 31 December 2017

| (in millions) | 2017 EUR | 2016 EUR | 2015 EUR | 2014 EUR | 2013 EUR |
|---|---|---|---|---|---|
| Operating revenue before rebate | **780** | 745 | 710 | 628 | 618 |
| Rebate | **–** | – | (33) | (31) | (34) |
| Revenue after rebate | **780** | 745 | 677 | 597 | 584 |
| Operating expenses | **(697)** | (691) | (653) | (559) | (546) |
| Profit before taxation | **69** | 47 | 35 | 38 | 35 |
| Net profit | **45** | 26 | 19 | 29 | 21 |
| Net cash flow from operating activities | **155** | 53 | 64 | 104 | 77 |
| Capital expenditure of which: | **80** | 51 | 48 | 38 | 46 |
| property, plant and equipment | **53** | 42 | 38 | 29 | 40 |
| intangibles | **27** | 9 | 10 | 9 | 6 |
| Shareholders' equity | **469** | 415 | 388 | 326 | 325 |
| Total assets | **804** | 797 | 763 | 714 | 603 |
| Number of employees at end of year | **2,779** | 2,629 | 2,328 | 2,163 | 2,010 |

To download the full set of financial statements, including the accompanying notes referred to below, please visit: www.swift.com

## Consolidated statement of comprehensive income

For the year ended 31 December 2017

| (in thousands) | | Note | 2017 EUR Before tax | 2017 EUR Tax (expense)/ benefit | 2017 EUR Net of tax | 2016 EUR Before tax | 2016 EUR Tax (expense)/ benefit | 2016 EUR Net of tax |
|---|---|---|---|---|---|---|---|---|
| **Profit for the year** | **(A)** | | **69,499** | **(24,380)** | **45,119** | 46,905 | (20,686) | 26,219 |
| **OCI items that may be reclassified subsequently to profit or loss:** | | | | | | | | |
| Foreign currency translation | | | **(1,419)** | **–** | **(1,419)** | (87) | – | (87) |
| Cash flow hedges: | | | | | | | | |
| Current year gain/(loss) on financial instruments | | 31 | **(5,504)** | **1,627** | **(3,877)** | 1,469 | (500) | 969 |
| Prior year (gain)/loss transferred to income statement | | 31 | **(1,469)** | **500** | **(969)** | 449 | (152) | 297 |
| **OCI items that will not be reclassified to profit or loss:** | | | | | | | | |
| Recognition of actuarial gains and losses | | 24 | **27,622** | **(15,301)** | **12,321** | (1,299) | (1,624) | (2,923) |
| **Other comprehensive income** | **(B)** | | **19,230** | **(13,174)** | **6,056** | 532 | (2,276) | (1,744) |
| **Total comprehensive income for the year** | **(A) + (B)** | | **88,729** | **(37,554)** | **51,175** | **47,437** | **(22,962)** | **24,475** |
| Attributable to: | | | | | | | | |
| Equity holders of the parent | | | | | **53,089** | | | 26,046 |
| Non-controlling interests | | | | | **(1,914)** | | | (1,571) |
| | | | | | **51,175** | | | 24,475 |

## Consolidated profit and loss statement

For the year ended 31 December 2017

| (in thousands) | Note | 2017 EUR | 2016 EUR |
|---|---|---|---|
| **Revenue** | | | |
| Traffic revenue | 2 | **357,259** | 347,235 |
| One-time revenue | 3 | **17,267** | 19,896 |
| Recurring revenue | 4 | **227,508** | 208,576 |
| Interface revenue | 5 | **175,940** | 167,088 |
| Other operating revenue | | **2,436** | 2,341 |
| | | **780,410** | 745,136 |
| **Expenses** | | | |
| Royalties and cost of inventory | 12 | **(7,038)** | (6,001) |
| Payroll and related charges | 6 | **(331,743)** | (352,982) |
| Network expenses | 7 | **(14,361)** | (13,840) |
| External services expenses | 8 | **(274,738)** | (263,765) |
| Depreciation of property, plant and equipment | 13 | **(46,459)** | (43,450) |
| Amortisation of intangible assets | 14 | **(11,630)** | (9,099) |
| Other expenses | 9 | **(10,850)** | (2,356) |
| | | **(696,819)** | (691,493) |
| **Profit from operating activities** | | **83,591** | 53,643 |
| Financing costs | 10 | **(1,287)** | (1,293) |
| Other financial income and expenses | 10 | **(12,805)** | (5,445) |
| **Profit before tax** | | **69,499** | 46,905 |
| Income tax expense | 11 | **(24,380)** | (20,686) |
| **Net Profit** | | **45,119** | 26,219 |
| Attributable to: | | | |
| Equity holders of the parent | | **46,554** | 27,924 |
| Non-controlling interests | 15 | **(1,435)** | (1,705) |
| | | **45,119** | 26,219 |

# Security audit and financial performance (continued)

To download the full set of financial statements, including the accompanying notes referred to below, please visit: www.swift.com

To download the full set of financial statements, including the accompanying notes referred to below, please visit: www.swift.com

## Consolidated statement of financial position

For the year ended 31 December 2017

| (in thousands) | Note | 2017 EUR | 2016 EUR |
|---|---|---|---|
| **Non-current assets** | | | |
| Property, plant and equipment | 13 | **193,207** | 186,890 |
| Intangible assets | 14 | **36,628** | 20,947 |
| Other investments | 16 | **250** | – |
| Deferred income tax assets | 17 | **36,887** | 74,392 |
| Other long-term assets | 21 | **12,969** | 15,739 |
| **Total non-current assets** | | **279,941** | 297,968 |
| | | | |
| **Current assets** | | | |
| Cash and cash equivalents | 18 | **294,659** | 219,049 |
| Other current financial assets | 18 | **74,000** | 132,000 |
| Trade receivables | 19 | **82,895** | 75,236 |
| Other receivables | 20 | **20,981** | 22,432 |
| Prepayments to suppliers and accrued income | 21 | **40,335** | 44,223 |
| Inventories | 22 | **1,645** | 2,245 |
| Prepaid taxes | 23 | **9,425** | 3,987 |
| **Total current assets** | | **523,940** | 499,172 |
| | | | |
| **Total assets** | | **803,881** | 797,140 |
| | | | |
| **Shareholders' equity** | | **469,330** | 415,332 |
| Equity attributable to equity holders of the parent | | **462,122** | 409,519 |
| Non-controlling interests | 15 | **7,208** | 5,813 |
| | | | |
| **Non-current liabilities** | | | |
| Long-term employee benefits | 24 | **104,597** | 160,895 |
| Deferred income tax liabilities | 17 | **3,765** | 5,913 |
| Long-term provisions | 26 | **18,721** | 11,594 |
| Other long-term liabilities | 27 | **215** | 471 |
| **Total non-current liabilities** | | **127,298** | 178,873 |
| | | | |
| **Current liabilities** | | | |
| Amounts payable to suppliers | 27 | **53,460** | 56,425 |
| Short-term employee benefits | 25 | **67,169** | 64,154 |
| Short-term provisions | 26 | **8,207** | 10,994 |
| Other liabilities | 27 | **73,319** | 65,040 |
| Accrued taxes | 28 | **5,098** | 6,322 |
| **Total current liabilities** | | **207,253** | 202,935 |
| | | | |
| **Total equity and liabilities** | | **803,881** | 797,140 |

## Consolidated statement of cash flows

For the year ended 31 December 2017

| (in thousands) | Note | 2017 EUR | 2016 EUR |
|---|---|---|---|
| **Cash flow from operating activities** | | | |
| **Profit before taxation** | | **69,499** | 46,905 |
| Depreciation of property, plant and equipment | 13 | **46,459** | 43,450 |
| Amortisation of intangible assets | 14 | **11,630** | 9,099 |
| Net (gain)/loss and write-off on sale of property, plant and equipment, and intangible assets | | **399** | 70 |
| *Other non-cash operating losses/(gains)* | | | |
| Increase/(decrease) in provisions, pensions and government grants | | **(20,657)** | (711) |
| (Increase)/decrease in other net long-term assets | | **2,514** | (7,963) |
| Net financial (income)/costs | | **1,306** | 1,829 |
| Net unrealised exchange (gain)/loss | | **(4,845)** | (707) |
| Increase/(decrease) in other non-cash operating items | | **(1,658)** | 3,096 |
| *Changes in net working capital* | | | |
| (Increase)/decrease in trade and other receivables and prepayments | | **(2,320)** | (31,056) |
| (Increase)/decrease in inventories | 22 | **600** | 505 |
| Increase/(decrease) in trade and other payables | | **5,313** | 5,775 |
| Investments in other financial assets | 18 | **57,750** | 591 |
| **Net cash flow before interest and tax** | | **165,990** | 70,883 |
| Interest received | | **828** | 671 |
| Interest paid | | **(2,084)** | (2,483) |
| Tax paid | | **(9,538)** | (15,773) |
| **Net cash flow from operating activities** | | **155,196** | 53,298 |
| | | | |
| **Cash flow from investing activities** | | | |
| Capital expenditures | | | |
| Property, plant and equipment | 13 | **(53,380)** | (42,074) |
| Intangibles | 14 | **(27,319)** | (8,558) |
| Proceeds from sale of fixed assets | | **213** | 886 |
| Capital increase in partly owned subsidiaries | | **3,309** | 4,002 |
| **Net cash flow used in investing activities** | | **(77,178)** | (45,744) |
| | | | |
| **Cash flow from financing activities** | | | |
| Net payments for reimbursement of capital | | **(470)** | (474) |
| **Net cash flow from/(used in) financing activities** | | **(470)** | (474) |
| | | | |
| **Increase/(decrease) of cash and cash equivalents** | | **77,548** | 7,080 |
| | | | |
| **Movement in cash and cash equivalents** | | | |
| At the beginning of the year | | **219,049** | 212,538 |
| Increase/(decrease) of cash and cash equivalents | | **77,548** | 7,080 |
| Effects of exchange rate changes | | **(1,938)** | (569) |
| **At the end of the year** | 18 | **294,659** | 219,049 |
| | | | |
| **Cash and cash equivalent components are:** | | | |
| Cash | 18 | **41,467** | 25,517 |
| Liquid money market products | 18 | **253,192** | 193,532 |
| **At the end of the year** | 18 | **294,659** | 219,049 |

# SWIFT offices

## Global presence

## 28 offices worldwide

## Connecting more than 200 countries and territories

### Americas

**Brazil**
Itaim Business Center, conjunto 52
Rua Iaiá, 77, Itaim Bibi
CEP 04542-060 São Paulo, Brazil
Tel: +55 11 3514 9004

**Mexico**
Paseo de la Reforma 342, 26 Floor
Col. Juarez
Mexico City, 06600, Mexico
Tel: +52 55 2881 6742

**United States – Miami**
600 Brickell Avenue, Suite 1800
Miami, FL 33131
Tel: +1 305 347 6700

**United States – New York**
7 Times Square
45th floor
New York, NY 10036
Tel: +1 212 455 1800

### Asia Pacific

**Australia**
Suite 2301, Level 23, 259 George Street
Sydney NSW 2000
Tel: +61 2 92 25 8100

**China, People's Republic of – Beijing**
Units 902-903, 9th Floor
No. 7 Financial Street
Winland International Finance Centre
Xicheng District
Beijing 100033, PRC

**China, People's Republic of – Shanghai**
Unit 4606-08
46/F IFC 2
8 Century Avenue
Pudong Shanghai China
200120
Tel: +86 21 8021 8000

**China – Hong Kong**
Suites 3201-09, 32/F
One Island East
18 Westlands Road
Island East, Hong Kong
Tel: +852 2107 8700

**India**
Unit No.1303, 13th Floor
The Capital, Plot No. C-70, G Block
Bandra-Kurla Complex
Bandra (East)
Mumbai 400 051
Tel: +91 22 6196 6900

**Indonesia**
45/F, Menara BCA Grand Indonesia
Jl.MH. Thamrin No.1
Jakarta, 10310
Indonesia
Tel: +62 21 2358 4400

**Japan**
20th Floor Nippon Life Marunouchi Building
1-6-6 Marunouchi
Chiyoda-ku
Tokyo 100-0005
Tel: +81 3 5223 7400

**Korea**
Jongno Tower Level 17
51 Jongno
Jongno-gu
Seoul 03161
Tel: +82 2 6353 4550

**Malaysia**
SWIFT Support Services Malaysia Sdn. Bhd.
Level 8, UOA Corporate Tower
Lobby B, Avenue 10, The Vertical
Bangsar South City,
No.8, Jalan Kerinchi
59200, Kuala Lumpur
Tel: +603 2778 7500

**Singapore**
8 Marina View
Asia Square Tower 1 #28-04
Singapore 018960
Tel: +65 6347 8000

### Europe, Middle East and Africa

**Austria**
SWIFT Austria GmbH
Regus Business Centre "Le Palais"
Herrengasse 1-3
1010 Vienna
Tel: +43 1 74040 2370

**Belgium**
Avenue Adèle 1
B-1310 La Hulpe
Tel: +32 2 655 31 11

**France**
Opera Trade Center
4 rue Auber
75009 Paris
Tel: +33 1 53 43 23 00

**Germany**
SWIFT Germany GmbH
City-Haus I, Platz der Republik 6
D-60325 Frankfurt am Main
Tel: +49 69 7541 2200

**Ghana**
SWIFT West Africa Limited
No. 31 Asafoanye O. Broni Crescent
Ringway Estates
Osu, Accra
Tel: +27 11 218 5363

**Italy**
6th Floor, Corso Matteoti 10
20121 Milan, Italy
Tel: +39 02 7742 5000

**Kenya**
Delta Corner
Chiromo Road, 07th Floor
Westlands 00800
Nairobi
Kenya
Tel: +254 730 11 2114
Tel: +27 11 218 5362

**Russian Federation**
LOTTE Business Centre
8, Novinsky Boulevard
121099 Moscow
Tel: +7 495 228 5923

**South Africa**
Unit 18, 2nd Floor
1 Melrose Boulevard
Melrose Arch
Gauteng 2076
Tel: +27 (11) 218 5353

**Spain**
Edificio Cuzco IV, 22nd floor – Paseo de la Castellana 141, 22B – 28046 Madrid
Tel: +34 91 425 1300

**Sweden**
P.O. Box 7638
Oxtorgsgatan 4, 7th floor
103 94 Stockholm
Tel: +46 8 508 95 300

**Switzerland**
Freischützgasse 10
8004 Zurich
Tel: +41 43 336 54 00

**United Arab Emirates**
DIFC – The Gate Village 5
Level 1
P.O. BOX 506575
Dubai
Tel: +971 4 4390870

**United Kingdom**
6th floor, The Corn Exchange
55 Mark Lane
London EC3R 7NE
Tel: +44 20 7762 2000

The list of SWIFT offices can change from time to time. Updated contact details for both our offices and for our Business Partners can be found at www.swift.com.

To view this Annual Review online, please visit:
**www.swift.com**


57371 – May 2018


This brochure is printed on Munken Polar – an FSC® Mix grade manufactured at a mill certified to ISO 14001 and EMAS environmental management standards. The pulp used in this product is bleached using both Elemental Chlorine Free (ECF) and Totally Chlorine Free (TCF) processes.

Printed by Pureprint. Pureprint are ISO 14001 certified, CarbonNeutral and FSC and PEFC Chain of Custody certified. The inks used are vegetable oil-based.