SWIFT

Annual Review

2016

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.

2016 highlights

100%

SWIFTNet availability

11,000+

institutions connected to SWIFT

200+

countries and territories

99.997%

FIN availability

100%

of services exceeded availability targets

6.5+ billion

total FIN messages

25.8+ million

average daily number of FIN messages

30.3+ million

FIN messaging peak day

+6.9%

FIN traffic increase

4.2+ billion

total FileAct traffic (Kchar)

16.8+ million

average daily FileAct traffic (Kchar)

+29%

FileAct growth (Kchar)

1.0+ billion

total InterAct messages

+71%

InterAct traffic increase

4+ million

average daily InterAct traffic

Chairman's letter

Yawar Shah
Chairman of the Board

Few events have challenged your cooperative and the transaction banking industry as severely as the sophisticated cyber attacks against member banks that occurred in 2016. Times like these are a true test of the resilience and strength of your cooperative, and I am happy to report that SWIFT's Board and Management stepped up to the task.

The Board and Management worked hard to identify and get ahead of this serious and organised threat, and set out a strategy to help define what the banking ecosystem needed to do to protect, detect and prevent these attacks. This involved identifying the threat patterns and taking actions to help customers protect themselves, as well as detect situations of compromise. This industry-wide approach is delivering results – substantial progress has already been made but both SWIFT and its customers must continue to take specific actions to stay ahead of future attacks and to minimise impacts if such events occur.

Even more than before, cyber security is a Board-level issue. The SWIFT Board, with its dedicated governance role, has both challenged and worked closely with Management to ensure significant investments continue to be made in cyber security to protect SWIFT and to help the banking community where it can. Management goals and incentives have been aligned with the cooperative's security targets and talent has been focused on addressing this key priority. The Board and its various committees will continue to dedicate significant time at regular and extraordinary meetings to review and assess the progress on SWIFT's end-to-end security strategy.

The Management team has acted with conviction, and has demonstrated strong leadership and rigour. Management also engaged specialist assistance where necessary to bring on board additional expertise. Our cyber adversaries are strong and sophisticated and we must keep ahead of them.

The security of the international banking system requires everyone to act: you, your counterparts and your communities.

SWIFT is doing its part. True to its community approach, SWIFT launched the Customer Security Programme (CSP) in 2016 to help tackle the cyber challenge. The CSP creates the framework for SWIFT to support its users in securing their infrastructure. Under the CSP, SWIFT set up a dedicated Customer Security Intelligence team to help customers with their post-incident investigations and facilitate intelligence sharing on attackers' modus operandi to help protect other institutions. Having time-critical intelligence is vital in helping to identify, mitigate or prevent fraudulent transactions and supporting the process to recover funds.

SWIFT will continue to engage with you, our community, as we roll out new components of the CSP. Last year we consulted the SWIFT community on a set of security controls that are being implemented now, and will become mandatory for all users. The introduction of these mandatory security controls creates a security baseline for all SWIFT customers, which is a significant step towards strengthening the security and protection of customers' local environments and collectively reinforcing the cyber resilience of the financial community.

Your collaboration, support and engagement on all initiatives under the CSP are essential in making the strongest possible impact in the fight against cyber fraud.

SWIFT also continued to successfully run the day-to-day business of our cooperative; SWIFT continued to advance its innovation agenda, and made good headway on the commercial initiatives set out in the *SWIFT2020* strategy. I am pleased to announce that SWIFT's financials are strong and the cooperative is well positioned to maintain its operational excellence while pursuing its strategic objectives (1) to grow and strengthen core messaging services, (2) to expand and deepen market infrastructures offerings, and (3) to build the financial crime compliance portfolio.

In 2016 SWIFT maintained the high security and reliability performance our community expects – an extraordinary feat in this challenging operating environment. At the same time, SWIFT delivered key components of the Australian real time payments infrastructure (AU-NPP) and made strong progress on FIN Renewal. SWIFT teams also worked tirelessly to prepare the global payments innovation (gpi) initiative for launch in early 2017.

SWIFT's financial crime compliance offering serves as a model to show how SWIFT's community approach addresses our members' challenges. SWIFT set out to help its members by making use of its central role in the financial system to develop a cooperative utility to reduce the inefficiencies of each institution working alone. Today SWIFT offers a comprehensive suite of compliance products and services that significantly reduce the cost of compliance for our users. By the end of 2016, users from more than 200 countries had signed up for The KYC Registry; almost 600 users had registered for our Sanctions Screening Service; nearly 40 financial institutions had signed up for the Compliance Analytics tool; and 25 had signed up for the Sanctions Testing service. In providing these important tools and working together with our customers, we improve efficiencies deliver a standardised global service and help to continue to build trust in the global financial system.

The success of SWIFT's compliance utility provides a blueprint for our global community to tackle the cyber security challenge. Throughout 2016 we called upon our community to cooperate and engage with us, and we will continue to do so in order to protect our industry. Your cooperation reflects the true strength of our community. Rest assured that we will not stand still, and we will continue to raise the bar in terms of security.

The road ahead will require continued leadership from SWIFT and the banking community. The cyber threat is real, serious, and here to stay and we must address it at the same time as meeting our daily obligations. The Board and Management will continue to work together to ensure SWIFT's uncompromising focus on security.

I want to thank the Board as well as the management team and the entire SWIFT staff for their perseverance and hard work. I remain dedicated and committed to serving you at this critical juncture in your cooperative's history.

Yawar Shah
Chairman of the Board
May 2017

CEO's letter

Gottfried Leibbrandt
CEO

2016 was a transformational year for SWIFT and its community. The Bangladesh fraud in early February brought the cyber threat right to the doorstep of the transaction banking community. While we have no indication that SWIFT's network or core messaging services were compromised, the episode represented a challenge to the security of our transaction banking community which we tackled head on.

In May 2016 we launched our Customer Security Programme (CSP) – a framework designed to support our users in reinforcing the security of their SWIFT-related infrastructure and strengthening their cyber risk management. We committed a large number of our best people, as well significant financial investments to this key programme.

In just under a year, we have achieved substantial results with the CSP. We have set up a Customer Security Intelligence (CSI) team to investigate reported cases; we have shared anonymised intelligence on the modus operandi to protect other users; we have enhanced existing security features in our own products; we have issued security updates to our interfaces; and we have regularly updated security guidance for customers.

Throughout the year we engaged with the SWIFT community at our events, including at our annual Sibos conference, keeping our users abreast of the evolving cyber threat, as well as our response to it. We consulted widely with our community on the new set of security controls for our users that we published in early 2017. We will continue to roll out new components of the Customer Security Programme and engage with our community as we do so.

Effective cyber risk management is a challenge which demands a multi-faceted approach. Given the interconnectedness of the financial industry, it is vital that concerted efforts are taken at both institution and community level around the world. I am certain that it is only by working together that we can protect the global financial system and turn this threat into a manageable nuisance.

At the same time, SWIFT continued to deliver on its day-to-day mandate. Operational availability performance during 2016 was strong; we achieved 100% availability for SWIFTNet and 99.997% availability for our FIN messaging service, against the backdrop of growing volumes and the FIN Renewal project. We continued to make strong progress on FIN Renewal throughout 2016 and it is set to be completed in 2017. Once finalised, FIN Renewal will allow us to provide the community with a more powerful and cost-efficient operating platform.

We also continued to roll out our *SWIFT2020* strategy with its focus on correspondent banking, financial crime compliance and market infrastructures, and we continued to support our customers with innovative new services. In 2016 we delivered several new components needed to build the real-time payments system in Australia (AU-NPP), and with the support of its participants, we completed the testing of the newly deployed local infrastructure. AU-NPP is on track and scheduled to be operational by the second half of 2017.

I am also particularly excited about the launch of the global payments innovation (gpi) initiative, and the potential benefits this will bring to our community. SWIFT's gpi promises to be truly transformational for the worldwide correspondent banking industry by offering a greatly enhanced service with increased speed, traceability, and transparency. It shows how SWIFT continues to innovate, providing our community with the means to meet their customers' evolving expectations. By the end of 2016, nearly 100 leading banks had signed up to the initiative. The gpi solution subsequently went live in January 2017 and hundreds of thousands of messages have since been successfully and securely delivered, across more than 60 country corridors.

In 2016 we also extended our financial crime compliance (FCC) offering, most notably by launching the Sanctions Name Screening service and Daily Validation Reports. By the end of the year, SWIFT's KYC Registry had more than 3,400 users.

In line with the increased threat, and reflecting our uncompromised focus on security, we have continued to invest in security and grow our dedicated staff; by the end of 2016 we had tripled the size of our security teams over the previous three years. We have bolstered our information security function by hiring a new Chief Information Security Officer (CISO) and creating new positions in the CISO office, enhancing the existing talent in this important part of our organisation. To ensure our own readiness to respond to unexpected threats, we also continued to test ourselves, carrying out more than 500 business continuity exercises during the year.

SWIFT continues to deliver and evolve, because of and in spite of the challenges and opportunities facing our cooperative. Our ongoing drive for improvement ensures that we continue to provide a secure and innovative service, setting the benchmark in the financial world.

I would like to thank the Board for their guidance during these challenging times, as well as Management and all SWIFT staff for their remarkable dedication. Their combined know-how and experience allowed us to respond to and support our community when it was most needed. We look forward to continuing to work closely with the community and to meeting when we gather at Sibos in Toronto in October 2017.

Gottfried Leibbrandt
CEO
May 2017

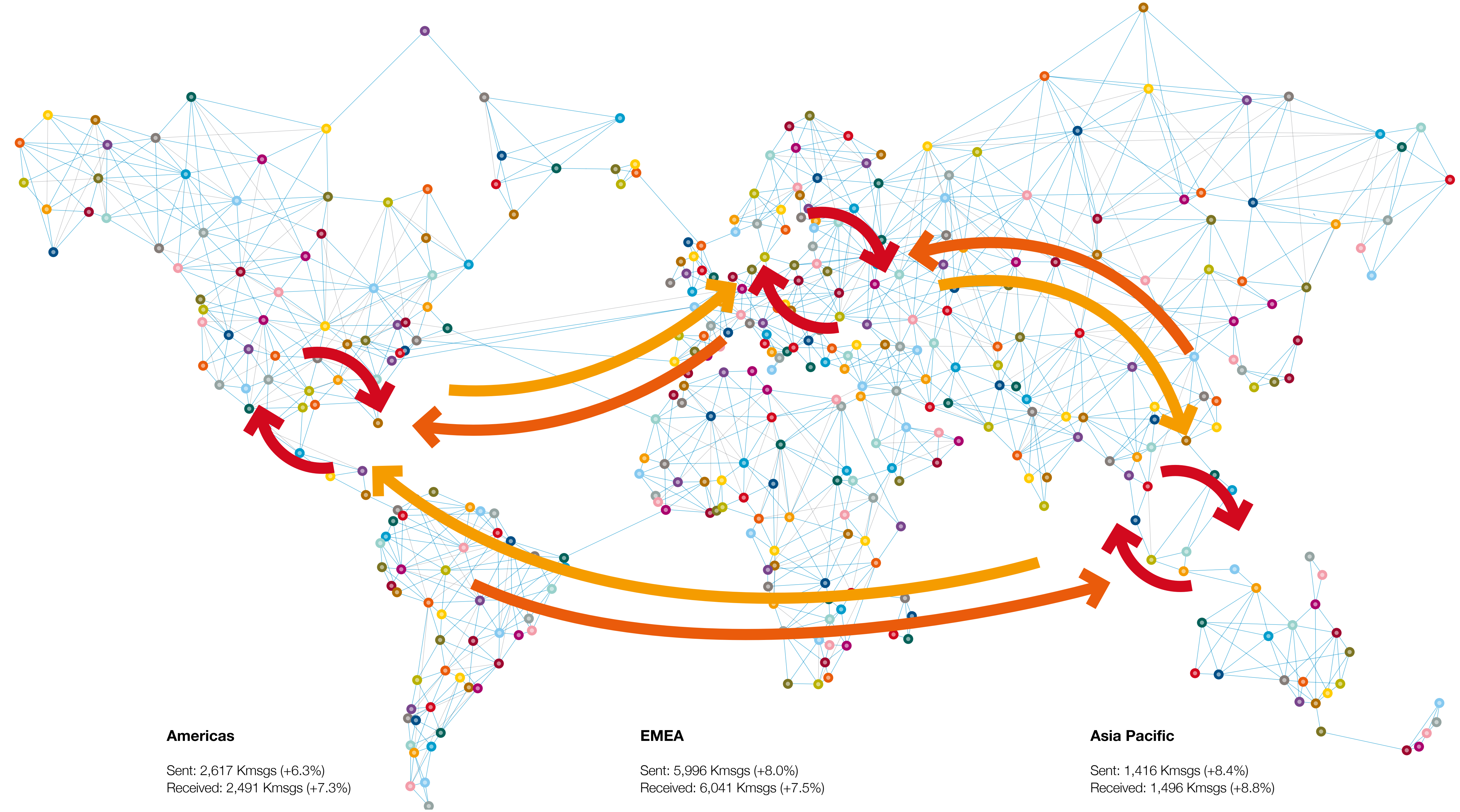
Payments regional traffic flows

This graphic compares year-on-year growth rates for regional payment flows in 2016.

During 2016 SWIFT observed traffic growth in all regions and for all routes between regions, except for traffic sent from Asia Pacific to EMEA. Traffic from EMEA to Asia Pacific, however, had the strongest inter-regional growth rate in 2016, increasing by 8.2 percent year-on-year.

Intra-regional growth was robust in all three regions, with Asia Pacific showing the strongest growth at more than 16 percent.

2016 average daily FIN messaging volume in Kmsgs (growth versus 2015)



Americas

Sent: 2,617 Kmsgs (+6.3%)
Received: 2,491 Kmsgs (+7.3%)

Intra-Americas:
1,153 Kmsgs (+8.1%)
Sent to Asia Pacific:
548 Kmsgs (+1.0%)
Sent to EMEA:
915 Kmsgs (+7.5%)

EMEA

Sent: 5,996 Kmsgs (+8.0%)
Received: 6,041 Kmsgs (+7.5%)

Intra-EMEA:
4,772 Kmsgs (+8.2%)
Sent to Asia Pacific:
288 Kmsgs (+8.2%)
Sent to Americas:
936 Kmsgs (+7.3%)

Asia Pacific

Sent: 1,416 Kmsgs (+8.4%)
Received: 1,496 Kmsgs (+8.8%)

Intra-Asia Pacific:
660 Kmsgs (+16.5%)
Sent to EMEA:
354 Kmsgs (-0.5%)
Sent to Americas:
402 Kmsgs (+4.9%)

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

Prioritising security and operational availability

Delivering value through FinTech innovation

Supporting increasing global messaging traffic

Committed to operational excellence

In 2016 SWIFT continued delivering on its commitment to reliability, from both a security perspective and from a service availability perspective. SWIFT achieved 99.997% availability for its FIN messaging service, and 100% for SWIFTNet. During the year all of our services exceeded their availability targets. At the same time our FIN messaging traffic continued to increase, growing to 6.5 billion messages during the year.

These excellent operational results are a result of our Failure is Not an Option (FNAO) mindset, our renowned security expertise and our IT security leadership, which position us to support the global financial industry in addressing its cyber security challenges.

We take great pride in our critical role in the global financial system and we continuously invest in technology, security, people and processes to ensure we deliver on our responsibility for operational excellence.

Security – what we do, who we are

In a rapidly changing threat landscape, we have further intensified our cyber security efforts. Building on our long-standing expertise in delivering secure products and services, and our unique role as central service provider, we have taken a leading role to help our financial community identify potential vulnerabilities and strengthen their cyber security. SWIFT's newly-formed Customer Security Intelligence team (CSI) brings together a strong group of IT and cyber experts to investigate security incidents within customer environments and to coordinate cyber intelligence sharing.

In 2016 SWIFT launched the Customer Security Programme (CSP), which leverages our community role to work with our users and help them address cyber security threats. The CSP is a dedicated initiative designed to reinforce and evolve the security of global banking, consolidating and building upon existing SWIFT and industry efforts.

SWIFT's Cyber Roadmap sets out our investments in our infrastructure and our people, reinforcing SWIFT's own defences in line with our strict risk management profile. SWIFT's 2016 Cyber Roadmap included initiatives to further enhance prevention, detection, response and recovery from cyber attacks against our own infrastructure. We carried out ethical hacking exercises to simulate malicious cyber attacks, and we tested and further improved our cyber readiness.

In 2016, we also continued enhancing our own products and services to provide additional protection and detection features to combat fraud and help customers protect their local SWIFT access points.

SWIFT's Security team has more than tripled in size over the past three years, and further growth is planned for the coming years. We have rolled out a 24/7 Security Operations Centre (SOC) whose mission is to actively monitor, detect and react to any logical or physical security attacks or threats. Security is the responsibility of each and every employee at SWIFT. Investments in dedicated security training and continuous emphasis on the security culture at all levels form another cornerstone of our success.

Track record in resilience

Our consistently high availability performance is the result of continuous investments in the technology, people and processes that underpin our core messaging service. 2016 availability for FIN and SWIFTNet, at 99.997% and 100% respectively, is testament to our commitment to delivering industry-leading availability.

On 30 June 2016 SWIFT recorded a new FIN messaging peak day, when 30,392,943 messages were sent over the network in a single day. We reached this new peak of more than 30 million messages only four years after crossing the 20 million message threshold in June 2012.

In addition to evolving our security processes, growing messaging traffic volumes and maintaining very high levels of availability and security, we continued to modernise and evolve our core platform. We made further progress on the FIN Renewal Programme which is now close to completion. The FIN Renewal Programme was initially launched in 2011 to make our messaging infrastructure more cost-effective and to further strengthen resilience and scalability. During 2016 we also improved the resilience of Alliance Lite2 by activating an additional disaster recovery site.

SWIFT's resilience is also the result of continuous testing and improvement. In 2016 SWIFT conducted more than 500 business continuity exercises, and carried out in-depth post-incident investigations and analysis for the rare events when a service was impacted.

Delivering innovative solutions

In 2016 SWIFT combined all Research and Development (R&D) activities in our IT and business development teams in an effort to optimise our business development structures. The result is a unified process across our product and service portfolio, with an emphasis on improving the customer experience through joint research and market analysis.

Examples of innovative new solutions that matured or went live in 2016 include the following:

- Our Financial Crime Compliance Portfolio was extended with new products and services such as Sanctions List Distribution, Payments Data Quality Financial Action Task Force (FATF) 16 Reporting, Online Name Screening, Daily Validation Reports and the KYC Adverse Media feed
- SWIFTSmart, our new eLearning platform, went live in November with close to 100 customers accessing the platform on the first day
- Roll-out of the Australian New Payments Platform (AU-NPP) for real-time payments is on track to go live
- The global payments innovation (gpi) initiative was completed ahead of its go-live in January 2016. SWIFT's gpi responds to evolving customer needs for greater speed, transparency and traceability in cross-border payments
- The development of a distinctive Distributed Ledger Technology platform which leverages our unique role in the financial industry to drive innovation and foster collaboration in new technologies

100%
SWIFTNet availability

99.997%
FIN availability

24/7
security operations

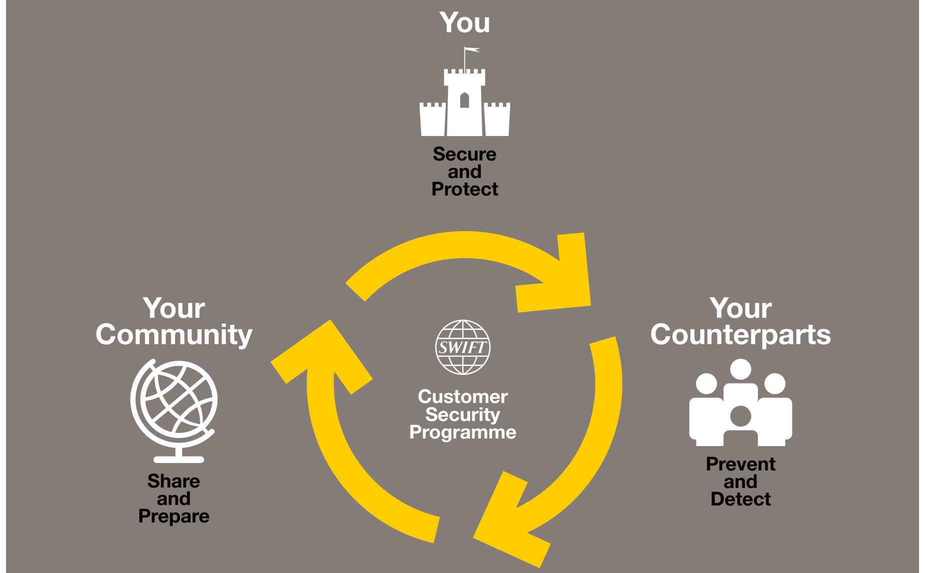
Customer Security Programme

Combatting cyber fraud in the financial industry

You: secure and protect your local environment

Your Counterparts: prevent and detect fraud in your commercial relationships

Your Community: continuously share information to prepare against future cyber threats



Combatting fraud is a challenge for the global financial industry, particularly in light of the increasingly sophisticated cyber threat landscape. In 2016 some highly publicised cyber attacks affecting a small number of SWIFT customers marked a watershed for the financial industry. These widely reported cases shed light on how sophisticated cyber criminals are now directly targeting banks' local infrastructures to effect input fraud.

There is no indication that SWIFT's network or core messaging services were compromised in any of these attacks. However, as a global cooperative, SWIFT is committed to supporting its customers and community in managing these cyber risks. To this end, SWIFT announced the introduction of its Customer Security Programme (CSP) in May 2016.

The CSP is articulated around three mutually reinforcing areas. Customers first need to secure and protect their local environment (You), prevent and detect fraud in their commercial relationships (Your Counterparts), and continuously share information and prepare against future cyber threats in collaboration with others (Your Community).

The SWIFT Board is working closely with management on the programme's development; and our overseers are monitoring the set-up and roll-out of the CSP.

Secure and Protect (You)

As a priority, customers should secure their own local environments, including the physical set-up of their local SWIFT-related infrastructure, and put in place the right people, policies and practices to avoid cyber-related fraud.

At Sibos, SWIFT announced plans to introduce a set of core security controls that all customers must meet to secure their local SWIFT-related infrastructure. Detailed draft security controls (16 mandatory and 11 advisory) were published at Sibos, following which there was a two-month period during which feedback was gathered from customers through National Member and User Groups across the world. Both the mandatory security controls and the assurance approach are designed to evolve in line with observed threats. In 2017 SWIFT will require customers to provide detailed self-attestation against the mandatory controls.

To facilitate users' readiness for the security requirements, SWIFT also introduced new security features to its software during 2016. In July SWIFT issued Alliance Access Release 7.1.20 and 7.0.70 with stronger default password management, enhanced integrity checking and in-built two-factor authentication (2FA) for Alliance Access clients that did not already have existing 2FA implementations.

During the year SWIFT also made detailed security guidance available for each of our interfaces, including expanded guidance for Alliance Access and Entry, for Alliance Lite2 and for certified third party interfaces. The guidance documentation includes instructions and best practice on how to protect users' local environments.

Prevent and Detect (Your Counterparts)

In addition to these security measures, it is important for customers to manage security risk in their counterparty interactions and relationships. In light of the heightened cyber risk environment, customers should mitigate risk to their own institution as well as the risks associated with breaches at their counterparties.

To support these efforts SWIFT developed new anti-fraud reporting tools. In December 2016 SWIFT introduced Daily Validation Reports, a secondary fraud control to check on the previous day's transaction activity and to provide a focused review of large, unusual and new payment flows.

SWIFT also launched a campaign to remind customers of the security-related benefits of its existing Relationship Management Application (RMA) tool. The RMA allows customers to select the correspondents they agree to receive payment instructions from. The campaign, which remains ongoing, focuses on how customers should use the tool to clean up dormant or unused RMA relationships that may represent an unnecessary risk, and encourages the use of RMA Plus, which allows more granular control by message type.

Market practice also has an important role to play in handling counterparty relationships. In late 2016 SWIFT therefore engaged with banks to understand their requirements for fraud prevention tools. We are evaluating the need for a new common solution, and we are working to understand the challenges associated with fraud operations and investigations. In December we published an information paper setting out how customers can mitigate fraud risk by strengthening their payment operations.

SWIFT has also been engaging with the community to understand requirements for other types of fraud prevention controls that might operate 'in-flight' within the network. Development plans for these controls will be defined and shared in 2017.

Share and Prepare (Your Community)

Just as the financial industry is global, so too are the cyber challenges it faces; what happens to one company in one location can easily happen to another elsewhere. Information sharing plays an important role in countering this threat and is therefore critical to protecting the community.

In July SWIFT engaged expert cyber security firms and created a dedicated Customer Security Intelligence team, bringing together a strong group of IT and cyber experts to investigate security incidents within customer environments. The expert firms complement SWIFT's in-house cyber security expertise and work closely with SWIFT's Customer Security Intelligence team to support SWIFT's customer information sharing initiative to help strengthen cyber security across the global SWIFT community.

Under the information sharing initiative SWIFT has since been sharing anonymised information about reported attacks with the community in a confidential manner, publishing details on the modus operandi used in known attacks together with related Indicators of Compromise (IoCs). The initiative has delivered concrete results by helping to detect and thwart attacks on other institutions. Customers can now easily subscribe to and receive SWIFT's latest operational security information through our expanded notification service.

Throughout this time, SWIFT has regularly informed its customers of relevant cyber intelligence, new market practices and security recommendations. SWIFT has also been building a Chief Information Security Officer (CISO) network and has engaged in bilateral CISO meetings to increase collaboration and information sharing.

SWIFT will continue to expand and develop existing information sharing channels and platforms to achieve effective and efficient information sharing. We are also engaging with vendors and third parties to secure the wider ecosystem. At the same time we expect customers to prepare themselves by reviewing and acting on the information and security updates we provide, and by ensuring that their institutions adopt the mandatory security requirements for their local SWIFT-related infrastructure.

Market infrastructures

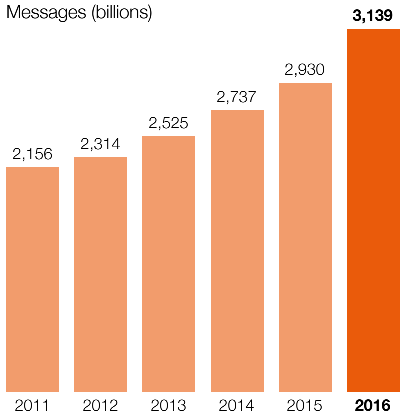
SWIFT's Market Infrastructures (MI) franchise now accounts for 35% of our messaging volumes, and a third of total revenue.

This success is a result of our focus and investments in MIs, which are strong drivers for innovation at SWIFT. Recent examples include SWIFT becoming a value-added network provider for TARGET2-Securities, developing an MI Gateway for Continuous Linked Settlement (CLS), and providing a shared back-up Real-Time Gross Settlement (RTGS) service through SWIFT's Market Infrastructure Resiliency Service (MIRS). MIRS is a fully diversified RTGS disaster recovery site hosted and operated by SWIFT. SWIFT also provides a messaging infrastructure for domestic payments in India, and we are on track to deliver a brand new real-time payments solution for Australia by the end of 2017.

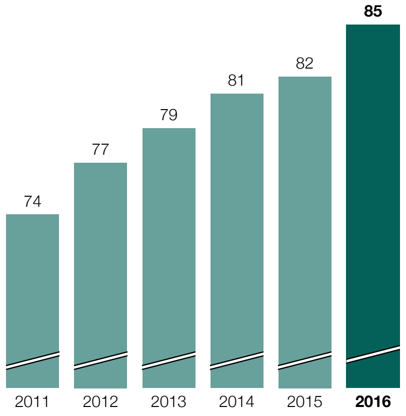
We expect the MI segment to continue making a significant contribution in the coming years. Not least because of the global adoption of ISO 20022, we see major shifts on the horizon for the very dynamic MI market segment.

Number of messages sent and received by MIs on SWIFT

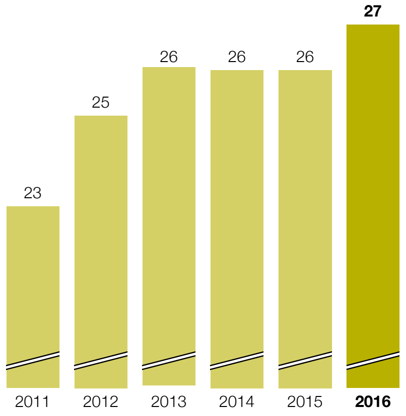
Messages (billions)



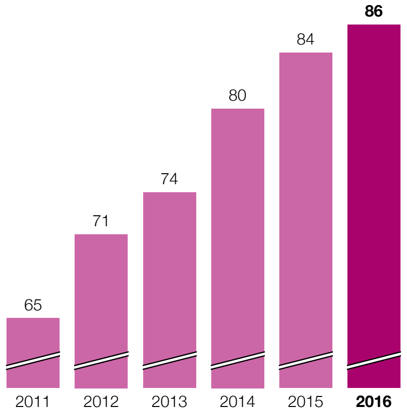
High value payment (HVP) systems connected to SWIFT



Low value payment (LVP) systems connected to SWIFT



Central securities depositories (CSDs) connected to SWIFT



2016 figures

778 million

HVP messages

90%

of TARGET2-Securities participants chose SWIFT as their network & messaging provider

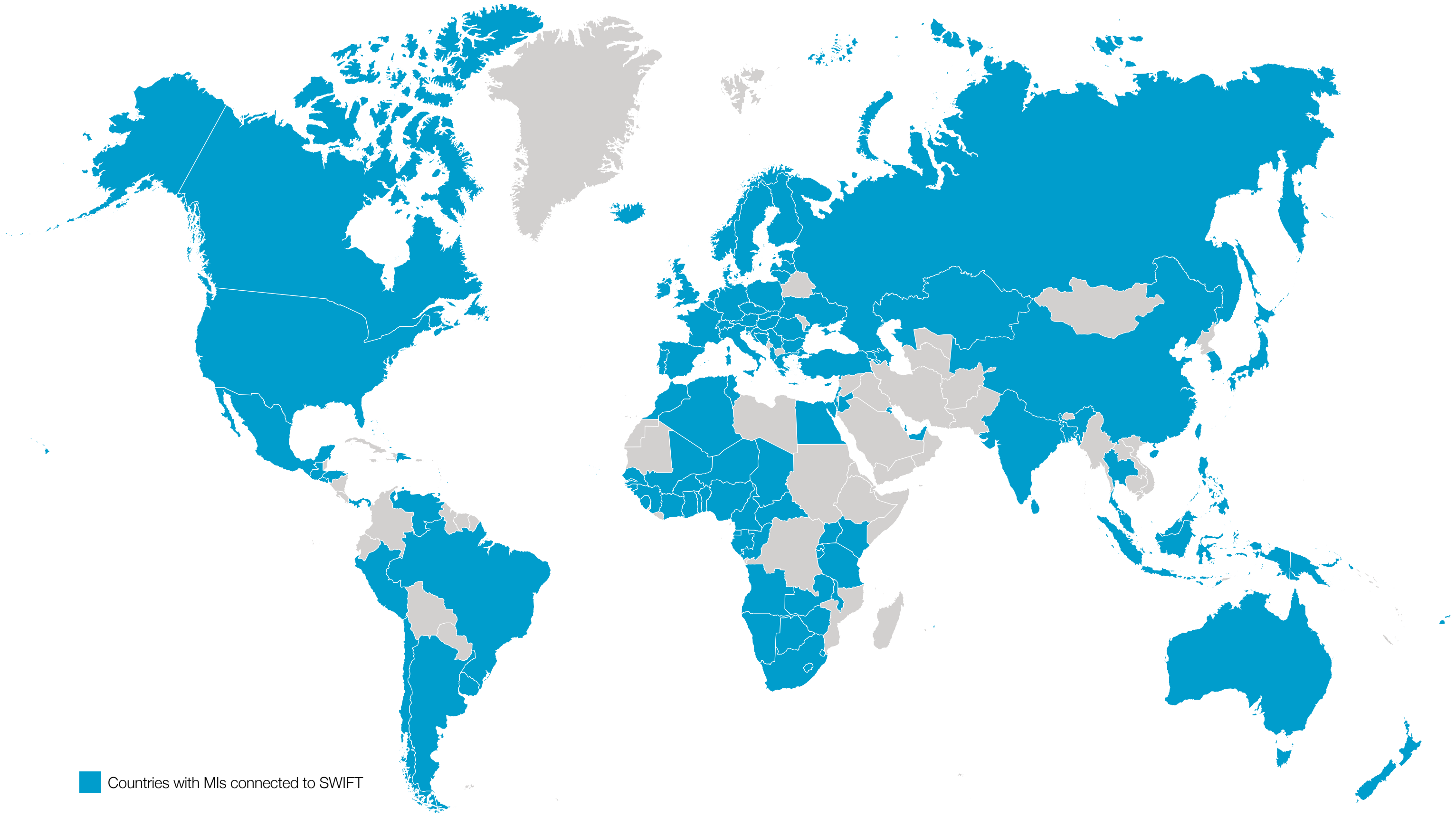
1.7 billion

CSD and CCP messages

252

live MI systems

122 countries with at least one market infrastructure connected to SWIFT at year end 2016



SWIFT worldwide

Achieving more together

Cooperating closely

Identifying challenges

Developing solutions

Shaping the future of the cooperative

SWIFT's events programme brought the community together during the year at regional conferences, standards forums, business and operational forums, and many open days. Our community engagement focused on the key theme 'Building the Future' and its three pillars: modernisation, innovation and inclusion.

APAC

SWIFT welcomed more than 2,600 customers at events across the Asia Pacific region. The Business Forum Malaysia in March was attended by 579 delegates and 43 speakers, and focused on FinTech, market infrastructure developments, and financial inclusion within the ASEAN region. The Business Forum Philippines welcomed 570 delegates and 42 speakers. In Mumbai, 246 attendees participated in the India and Subcontinents Regional Conference to discuss regional connectivity amongst the SAARC region (South Asian Association for Regional Cooperation) through harmonisation and use of global communication standards along with common infrastructure. At the Greater China Conference in Shanghai, 275 community members gathered to discuss RMB internationalisation and China's Cross-border Interbank Payment System (CIPS). While Macau celebrated its 30th anniversary of SWIFT connectivity, a series of other forums took place in Taiwan, Thailand, Japan and Korea. SWIFT presented a number of research papers at these events, covering the modernisation of the Philippines Financial Markets through ISO 20022; digitalisation; innovation; the globalisation of Japan's payments systems; and the internationalisation of the RMB.

EMEA

SWIFT brought together close to 4,500 financial industry experts across the EMEA region in 2016. Four hundred delegates from 48 countries joined us in Mauritius for the African Regional Conference (ARC), where sessions focused on the future of payments, financial crime compliance and cyber security. The ARC 2016 also saw the launch of the African Advisory Group (AAG). Composed of key industry players from across the region, the AAG aims to provide insights into the challenges and opportunities facing the African financial markets. At the ARC we also hosted the second Innotribe Startup Challenge for Africa.

The SWIFT Operations Forum Europe (SOFE) took place in Berlin and brought together more than 350 operational experts to learn, network and share best practices. Cyber security and the Customer Security Programme were top of the agenda. Business Forums in Benelux, Frankfurt, Milan, Moscow, Lisbon, South Africa, West Africa and the UAE meanwhile looked at the key trends in each market and what SWIFT is doing to support local communities. Many of these events also featured demo zones allowing delegates to experience our products and services at first hand, and to learn more about the ongoing R&D being carried out by SWIFT.

The SWIFT Business Forum London, SWIFT's largest regional event, took place in April and welcomed 1,200 people. Content was delivered across three streams – payments, securities and technology – and featured international industry thought leaders from banking and FinTech including Eileen Burbidge, the UK Treasury's FinTech adviser.

At the Nordics Regional Conference in March, 300 people joined us in Oslo to discuss how new technologies, changing business models and collaboration may impact the Nordics region in the coming years.

Americas

In April SWIFT hosted the Business Forum Canada, which brought 300 attendees together in Toronto to focus on payment systems modernisation. In May the 10th annual SWIFT Premium Services Forum was held in New York, with debate focused on key issues such as security and compliance. In June SWIFT hosted the Latin America Regional Conference in Mexico City, attended by 400 people from 20 countries. The event was also host to the first Innotribe Startup Challenge in the region, which brought together FinTech startups from across Latin America to showcase innovation.

To close the year, SWIFT hosted a number of 'SWIFT on…' events in London and New York in partnership with the Financial Times examining innovations in cross-border payments.

Innotribe

2016 was a successful year for Innotribe, with the start of a number of new partnerships and a series of community events held in different regions. Innotribe leveraged its Startup Challenge to support emerging FinTech ecosystems and introduced the Industry Challenges initiative. Innotribe was also instrumental in supporting the launch of the Global FinTech Hub Federation, a network of emerging and established FinTech hubs, in partnership with UK-based Innovate Finance. Innotribe continued to support research cooperation with proven FinTech firms, academics and leading industry experts.

Standards

In 2016 SWIFT organised Standards Forums and ISO 20022 events in New York, London, Zurich, Kuala Lumpur and Manila, culminating in the Sibos Standards Forum in Geneva. SWIFT Standards events were attended by over 2,500 guests and featured contributions from more than 150 industry speakers.

Throughout the year, the Standards team continued its mission to harmonise the implementation of ISO 20022 by market infrastructures (MIs). Together with 24 key members of the MI community, SWIFT formulated and agreed a new Standards management policy aimed at reducing the number of message versions in live operation; more MIs signed the ISO 20022 Harmonization Charter (30 in total); and new global market practice guidelines were agreed for important use-cases, including high value Real-Time Gross Settlement payments.

Standards also contributed to the emergence of Distributed Ledger Technology (DLT) in the financial industry by publishing an information paper on the application of business standards to DLT and developing, in collaboration with the Innovation team, a DLT proof of concept to automate the lifecycle of a fixed-rate bond.

SWIFT's MyStandards platform for sharing industry specifications reached over 20,000 individual users in 2016. Version 2.1 of the platform was launched in December, including significant new features for version management, search and batch operations.

SWIFT Institute

In 2016 the SWIFT Institute expanded its library of research by publishing six research projects. The SWIFT Institute has issued 34 research grants and published 24 papers since 2012.

The SWIFT Institute launched its first UK Student Challenge supported by the UK Treasury. Students were asked to solve a real world problem, and the winning team was selected by the attendees of the SWIFT Business Forum London. In April the SWIFT Institute held its first SWIFT Institute Talks, featuring presentations from speakers on topics such as regulation, cyber and blockchain.

The SWIFT Institute invited academics to speak at SWIFT regional conferences and business forums, including the Greater China Conference. At Sibos, the Institute had a dedicated stage on the SWIFT Stand, and showcased nine presentations on topics such as artificial intelligence in cyber security (by MIT) and the Impact of Open APIs on Banking (Warwick Business School). In November the Institute held its own conference on Digital Disruption in Financial Services in Toronto.

SWIFTLab

Throughout the year SWIFTLab enabled SWIFT to engage with its user community on topics related to innovation and R&D. Four new SWIFTLabs opened in Hong Kong, New York, London and Paris, and SWIFTLab showcased SWIFT products and innovation at the Business Forum London, SWIFT Operations Forum Europe and Sibos. At Sibos, SWIFTLab held 27 live sessions and welcomed over 1,200 visitors to discover SWIFT's future products and R&D activities, with a particular focus on the gpi payment tracker and SWIFT's latest proof of concepts on blockchain technology.

Sibos

Sibos 2016 was held in Geneva where 8,317 delegates from 145 countries gathered and a record high number of 201 exhibitors showcased their products and services. Cyber security, compliance, payments modernisation and cognitive intelligence were among the big topics on the conference programme, which also featured a range of industry-specific forums and more than 270 sessions with more than 580 speakers. Captains of industry including Ginni Rometty, CEO of IBM, and global thought leaders, such as cybersecurity expert Marko Gercke, shared their views on industry challenges and how to address them.

Growing and strengthening our core messaging services

Expanding and deepening our MI offerings

Building our financial crime compliance portfolio

Enabling growth

The *SWIFT2020* strategy sets out an ambitious agenda to 'grow the core, build the future' over the next five years. The strategy combines our continued focus on operational excellence and the strengthening of our core messaging business with significant areas of innovation to meet the changing needs of the global SWIFT community.

2016 marked the first full year of execution against the activities identified under *SWIFT2020*'s three strategic pillars: to grow and strengthen the core; to expand our MI offering; and to build our financial crime compliance products and services.

Grow and strengthen core messaging services for payments and securities

Our community places its trust in the security, reliability and availability of our messaging services. The *SWIFT2020* strategy addresses this through strategic investments in technology, security, people and processes.

During 2016, we:

- Implemented our strategy to grow our offering of interface and connectivity solutions, principally the Alliance Messaging Hub, which supports larger volume customers, and Alliance Lite2, a cloud-based solution for lower volume customers. We also delivered new security features for our interface products
- Continued to deliver on the FIN Renewal migration, to offer a more powerful and cost-effective platform for our FIN messaging service
- Successfully evolved our global payments innovation (gpi) initiative in response to the industry's call to revitalise correspondent banking. Designed as a key part of our 2020 strategy, near to 100 banks had signed up as members by the end of 2016 – representing 75% of SWIFT's messaging traffic
- Reviewed blockchain to better understand its relevance to the community. We also launched a number of proofs of concept investigating new ways to re-energise correspondent banking and help securities markets better manage post-trade risks. Innotribe's ongoing engagement with the FinTech start-up ecosystem was core to this activity.

Expand and deepen offerings for market infrastructures

In addition to our core 'many-to-many' messaging business, market infrastructures are an important segment in *SWIFT2020*. We have continued to support our user community with major structural and regional initiatives across securities and payment MIs. We have successfully grown the use of SWIFT among high value payment systems and central securities depositories, and continued leveraging ongoing projects such as CLS and TARGET2-Securities.

Key achievements also included:

- An expanded resilience service offering, building on the success of our Market Infrastructure Resiliency Service (MIRS)
- The development of the foundation components for the Australia New Payments Platform (AU-NPP), a new infrastructure for real-time payments set to go live in 2017
- Continued support of the global harmonisation of ISO 20022, supporting the community with a more streamlined transition to the new standard.

Build our financial crime compliance portfolio

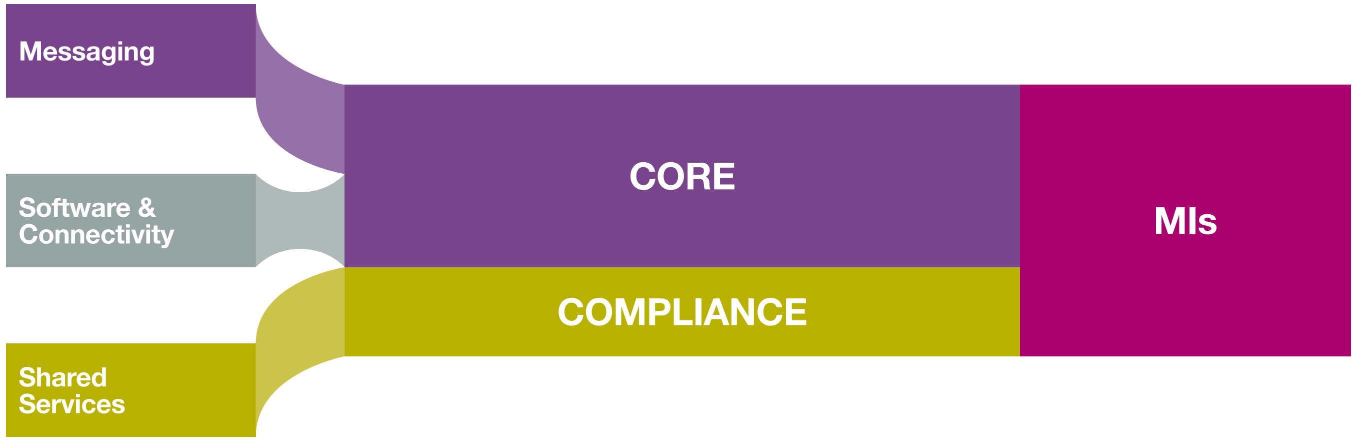
Given the extent of regulatory challenges across the industry as a whole, our 2020 strategy recognises the community-wide need for an extended financial crime compliance offering. We deepened and broadened our financial crime compliance portfolio in 2016 by introducing the Payments Data Quality and the Name Screening services. We also expanded our portfolio in the areas of Sanctions Screening and Testing products, the KYC Registry and Compliance Analytics.

Enabling growth

SWIFT2020 is a growth strategy set against the backdrop of rapidly changing industry conditions. As such, it supports our response to new challenges, such as those linked to cyber security. Launched in 2016, our Customer Security Programme (CSP) provides a framework to support our user community in securing the international financial system.

We have continued to strengthen our presence with our members across our community. We grew our network of SWIFTLabs to include the USA, Hong Kong, London, Singapore and Kuala Lumpur. With customer-centricity as one of our central principles, *SWIFT2020* lays the groundwork for our ongoing dialogue and engagement with our community at Sibos, the SWIFT Institute and the Standards Forum, as well as through our network of National Member and User Groups, consultative groups and national and regional business forums and events.

***SWIFT2020* – Strategic priorities**



SWIFT global payments innovation (gpi)

In January 2016 the SWIFT global payments innovation (gpi) initiative was announced, with 45 leading banks signed up from the outset. The initiative aims to significantly improve corporate treasurers' cross-border payment experience by increasing the speed and transparency of payments, as well as enabling end-to-end tracking.

Early adopting banks agreed a multilateral service level agreement (SLA) rulebook, and 21 gpi member banks participated in the pilot phase that commenced in mid-February 2016. The gpi pilot concluded in December 2016 with all participants successfully testing the design and core functions in bilateral exchange with SWIFT and with each other. In parallel, gpi banks not able to join the pilot were offered an on-boarding process to ensure they could prepare for live operations by January 2017.

Concurrently SWIFT developed a cloud-based payments tracker, a member directory and SLA observer to ensure that the new service meets transparency and traceability requirements. In addition, SWIFT actively worked with key payments market infrastructures worldwide to ensure end-to-end clearing and traceability of gpi cross-border payments, with the end-goal of achieving interoperability between domestic and international payments.

SWIFT also formed a gpi Vision Group, made up of leading gpi transaction banks, in order to advise on the future strategy for SWIFT gpi. In consultation with the Vision Group, SWIFT has identified the following optional payments services to digitally transform the cross-border payments experience:

- A stop and recall payment service offering banks the ability to stop payments no matter where they are in the correspondent banking chain
- A payment data transfer service to enable rich data to be sent along with payments
- An international payment assistant service to help corporates initiate error-free cross-border payment instructions.

These services will be designed, built and tested in 2017 and will go live in 2018, bringing additional value to the gpi platform.

In 2016 SWIFT and the Vision Group also scoped the potential of distributed ledger technology (DLT) to improve the cross-border payments process. It was determined that the reconciliation of banks' nostro accounts would be the most promising area to explore the application of DLT. Successful deployment of the ledger in this area could, potentially, allow for real-time reconciliation and the optimisation of banks' global liquidity. In January 2017 SWIFT announced, along with a number of gpi banks, the launch of a proof of concept to explore the potential of using DLT in this area. The proof of concept will be completed in July 2017 and the results will be presented at Sibos in October.

Throughout 2016 SWIFT gpi rapidly gained traction with nearly 100 member banks having signed up by December, representing 75% of all SWIFT cross-border payments. The momentum continues to build with global transaction banks starting to actively use the SWIFT gpi service in January 2017.

SWIFT gpi: delivering the future of cross-border payments, today

- **Nearly 100 member banks**
- **Hundreds of thousands of gpi messages already exchanged**
- **60+ country corridors covered**
- **21 banks successfully piloted**

Financial crime compliance

Financial institutions have invested heavily in systems and people to address rapidly changing regulatory compliance. As banks aim to rein in compliance costs, SWIFT is playing an active role by delivering hosted utility services that increase standardisation, are developed through collaboration, and mutualise and reduce costs for its members.

At Sibos 2016, senior compliance experts stated emphatically that utilities will play a major role in reducing the burden and delivering the benefits of effective and efficient compliance programmes. They singled out The KYC Registry, with more than 3,400 member banks, as establishing the benchmark for compliance utilities by providing a single, global source of standardised Know Your Customer information for SWIFT's correspondent banking community. KYC Registry adoption continues to be strong, and Registry membership will increasingly play a role in promoting transparency and enabling banks to address the challenges posed by de-risking activities.

In addition to KYC, SWIFT has invested heavily in developing sanctions compliance services. With nearly 600 user institutions signed up to the service, Sanctions Screening has validated the benefits of hosted screening services and paved the way for SWIFT's new Name Screening service which went live at the end of 2016. Name Screening addresses the need for banks and corporates to screen individual names and entire databases to support sanctions compliance, and gives SWIFT an end-to-end screening utility service. Rounding out the portfolio, Sanctions Testing is used by the majority of the world's largest banks – and SWIFT's largest customers – to provide third-party assurance and improve the performance of their sanctions screening systems.

In 2016, as part of its Customer Security Programme, SWIFT introduced Daily Validation Reports to help smaller banks identify potential fraud. Designed to complement customers' existing fraud controls, Daily Validation Reports use SWIFT's records of customers' transaction activity to provide an accurate means for them to verify their own messaging activity and identify suspicious transactions. The Daily Validation Reports are part of SWIFT's Compliance Analytics portfolio, which already enables about 40 of SWIFT's largest customers to analyse their global SWIFT traffic data to identify, monitor and address compliance risk. Compliance Analytics also helps banks strategically manage their Relationship Management Application (RMA) and RMA Plus business relationships to prevent unauthorised activity. With the EU Funds Transfer Regulation to take effect in 2017, SWIFT introduced a Payments Data Quality service to help banks comply with new requirements for originator and beneficiary information in payments messages. Not only does Payments Data Quality help customers comply with Financial Action Task Force (FATF) Recommendation 16, but it also helps banks improve overall data quality, supporting more effective compliance processes, straight-through processing and payments efficiency.

In 2017 SWIFT will continue to expand its financial crime compliance portfolio in line with its community's evolving needs. SWIFT will continue its *SWIFT2020* strategy to deliver interconnected utilities in the areas of KYC, anti-money laundering (AML) and sanctions, reducing overall cost for the industry, increasing transparency and supporting global business development and financial inclusion.

The KYC Registry: A secure, shared platform to exchange standardised Know Your Customer data

More than 3,400 institutions worldwide are using The KYC Registry

- **1,800+ in Europe, Middle East and Africa**
- **980 in Asia Pacific**
- **600+ in Americas**

Corporate social responsibility

Operating responsibly and sustainably

Caring for our communities

Facilitating business sustainability

24%

of SWIFT staff engaged in CSR activities

102,000 km

commuted by bicycle as part of the Bike to Work programme in Belgium

120,000

trees planted in India

34.1%

of people working at SWIFT are women

24.6%

of managers are women

In 2016 SWIFT made good progress 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), which we subscribed to in 2012 and have supported ever since.

Operating responsibly and sustainably

SWIFT aims to operate responsibly and sustainably. Reducing our impact on the environment and increasing diversity and inclusion within our company were among our top CSR goals in 2016. We extended these objectives to our suppliers and CSR partners by including our sustainability policy in all our contracts.

Greening SWIFT

Throughout 2016 SWIFT continued to implement measures aimed at reducing our cooperative's carbon emissions. We used renewable energy wherever feasible and we compensated carbon emissions caused by work-related travel and events. We carried out waste sorting and waste reduction campaigns, and promoted environmentally friendly behaviour among staff and contractors.

Offices and Data Centres

In 2016 we expanded our hot-desking programme to more SWIFT offices around the world, allowing us to further rationalise office space and control electricity consumption even while staff numbers continue to grow. We also replaced many old lamp bulbs with LED lighting. At our data centres we optimised the cooling systems and launched recycling programmes for electronic and paper products. SWIFT continued to promote the use of electric and hybrid cars amongst staff. We installed additional electricity plug-in stations in Belgium, The Netherlands and the US. As a result, SWIFT's average CO_2 company car emissions fell by 20% between 2011 and 2016. For the third year in a row, SWIFT was awarded the 5-star label from Tous vélo-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 102,000 km by cycling to work.

Sibos

At Sibos SWIFT initiated a number of 'green' measures in the areas of waste management, water consumption, biodiversity, recycling and use of public transport. SWIFT's conference stand used environmentally friendly materials including repurposed furniture, electrical fittings, wiring and audio-visual equipment. The exhibition manual was digital only, and delegates were able to offset their carbon emissions caused by air travel to and from the conference. SWIFT purchased carbon credits to support emission reduction projects which distribute modern, low-cost, fuel-efficient cooking stoves to private households in Ghana and Kenya.

Biodiversity

Protecting biodiversity is important to SWIFT. In 2016 the three beehives located at our headquarters produced 80 kg of honey. The proceeds from the sale of honey were donated to local bee protection associations.

SWIFT financed the planting of 120,000 trees in partnership with WeForest in India, an NGO devoted to reforestation of bio-diverse and indigenous forests in tropical countries, while providing jobs for women and enabling them to send their children to school.

Diversity and Inclusion

In 2016 we continued our journey towards more diversity and inclusion. Approximately 80% of our managers worldwide followed an unconscious bias workshop. The workshop is now part of the official training path for all newly appointed managers. SWIFT also launched Balance@SWIFT, an internal network through which staff bring up and discuss topics on diversity and inclusion, and can be inspired by internal and external role models.

At Sibos in Geneva, we organised diversity and inclusion sessions on two main topics:

- Engaging men in discussions about diversity and inclusion
- How diversity and inclusion helps people and businesses take better business decisions.

Finally, the SWIFT Executive Committee participated in an inclusive leadership workshop showing their engagement and commitment towards SWIFT's diversity and inclusion goals.

Caring for our communities

Nearly one in four SWIFT staff globally engaged in local CSR activities in 2016. Among others, staff participated in Team with Spirit events; donated blood; ran, cycled or walked for a charity; donated toys and Thanksgiving food baskets; visited hospitals; organised fundraising initiatives for disabled children; and tutored refugees. 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-standing partner, United Fund for Belgium, a non-profit organisation which distributes 100% of its donations to small charities involved in child welfare, poverty reduction, support for disabled persons and social integration and training.

Children in need and Education

In 2016 we continued our ongoing partnership with Teach for Belgium, an association that addresses educational inequality by training teachers to better support their students. In addition, SWIFT financially supported WAPA International and the Digital Leadership Institute. WAPA International raises funds to support local organisations helping to reintegrate child victims of war. The Digital Leadership Institute promotes greater participation of girls and women in strategic, innovative ESTEAM (entrepreneurship, science, technology, engineering, arts and mathematics) sectors. Additionally, SWIFT supported local charities supporting people in need in the regions in which we hosted regional conferences and business forums. In 2016 we selected ECPAT in Norway, Working Well Trust in the UK, the Daily Bread Food Bank in Canada, NorSA in South Africa and SOS Children's Villages in China, Germany, India, Italy, Mauritius, Mexico City, Nigeria, the Philippines, Portugal, Romania, Russia, Syria, Taiwan and Ukraine.

Humanitarian support

In 2016 SWIFT made substantial donations to the Red Cross to help Syrian war victims. We also supported victims of Hurricane Matthew in Haiti and the earthquake in Italy through direct donations and by supporting Doctors without Borders and Save the Children.

Facilitating business sustainability

In 2016 SWIFT developed and promoted partnerships with organisations supporting education, microfinance and financial inclusion in emerging countries, reinforcing our links with local communities in line with SWIFT's strategy and business priorities.

SWIFT continued to support education through the Nairobits Trust in Kenya, training less privileged young people in web design, IT and creative multimedia, helping them to enhance their employment and entrepreneurship opportunities. We expanded our partnership with the Teach for All network by financially supporting projects in Argentina, Bangladesh, Columbia, Ghana, and Nigeria. The projects aim to reduce education inequities through the development of transformational leadership programmes.

Financial education and inclusion are at the heart of SWIFT's educational support. SWIFT supported the Phakamani Foundation in South Africa and the Mann Deshi Foundation in India with grants, and we extended our partnership with Fundación Capital to finance the development and launch of tablet-based financial education apps aimed at supporting young people and women in Brazil, Mexico, Peru and Tanzania.

Throughout 2016 SWIFT facilitated dialogue on CSR issues within its community. The SWIFT Institute financed a research grant on financial inclusion in Kenya and provided a platform for discussion on the same subject at Sibos in Geneva.

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

Messaging facts and figures

FIN

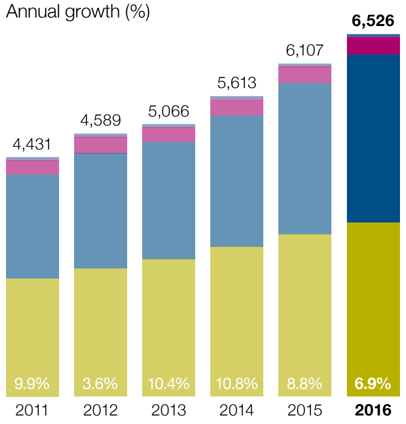
Financial institutions use FIN for individual, richly-featured messaging which requires the highest levels of security and resilience. Features include validation to ensure messages conform to SWIFT message standards, delivery monitoring and prioritisation, message storage and retrieval.

In 2016 more than 6.5 billion FIN messages, or an average of 25.8 million messages per day, were sent over SWIFT, representing a 6.9% increase over 2015.

SWIFT recorded three FIN peak days in 2016. The latest FIN peak, on 30 June, registered 30.3 million messages. It was driven by an end-of-month/quarter peak in payments traffic, combined with a Brexit-related surge in securities and treasury traffic. For the first time since 2011, SWIFT recorded two treasury peak days in a single year. The first one, in June, was linked to the Brexit decision; and the second, in November, at close to 2 million messages, followed the US Presidential election.

FIN messages – growth

Messages (millions)
Annual growth (%)



FIN share by market

2016 volume (millions)

● Payments[1]	3,139
● Securities	3,019
● Treasury	314
● Trade	37
● System	16

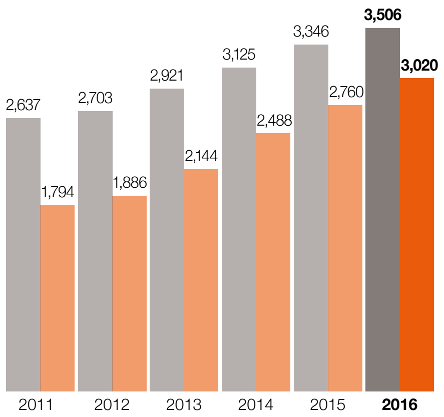
[1] including FIN Copy messages

Reporting messages versus non-reporting messages

Messages (millions)

● Non-reporting

● Reporting

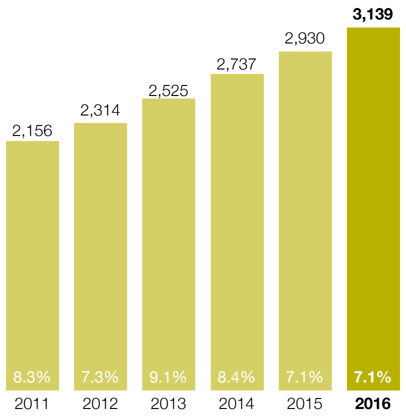


Reporting messages

Reporting messages grew by 9.4% during the year, outperforming non-reporting messages which grew by 4.8%. Over the last five years, the weight of reporting messages in total FIN traffic increased from 40% in 2011, to 46% in 2016.

Payment messages

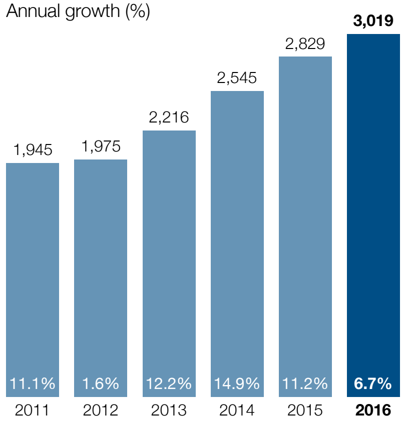
As the main driver of the 2016 growth, Payments messaging traffic grew by 10% during the year. Reporting messages now represent 46% of total Payments traffic. As usual the highest volumes were recorded in December, when Payments volumes reached an average of 13.8 million messages per day. Three new Payments traffic peaks were recorded in 2016, the last on 30 June, when there was a peak of 14.9 million messages.



Securities messages

For the first time since 2012, growth in Securities traffic was lower than Payments messaging growth. Similar to the Payments market, Securities reporting messages were a key contributor to growth. Some FIN Securities traffic was migrated to InterAct and FileAct as a result of TARGET2-Securities waves 1 and 2.

Messages (millions)
Annual growth (%)



FileAct

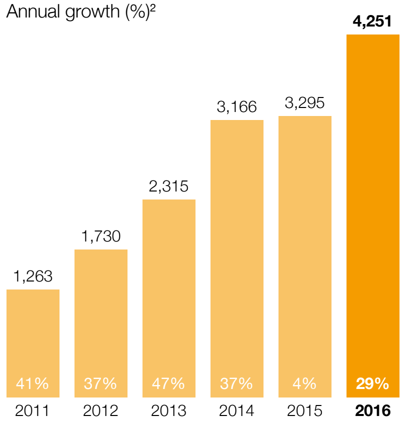
FileAct is an advanced, secured and resilient file transfer protocol tailored to customers' need to exchange freely formatted transactions in bulk mode. It is primarily used to exchange large batches of low value payments and the corresponding reporting.

At 29% FileAct traffic recorded strong double digit growth in 2016. Gains in the European card clearing business were the main driver behind this solid performance. TARGET2-Securities traffic was also a key contributor to 2016 growth, as further migration waves continued to unfold. The Corporates segment showed another year of steady traffic growth (23%).

FileAct volume in billions of characters	4,251
FileAct volume in million of files	125
Live and pilot users	2,782
Services using FileAct	177

FileAct traffic evolution

Number of characters (billions)
Annual growth (%)[2]



[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.

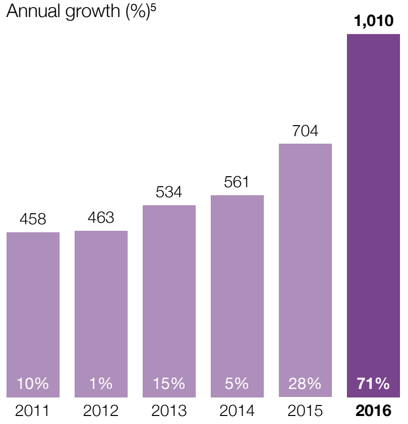
TARGET2-Securities was the key driver for InterAct traffic growth in 2016, as wave 2 and wave 3 of the migration went live during 2016. Over the full year, TARGET2-Securities InterAct traffic represented 44% of total InterAct traffic.

InterAct messages[3]	1,010 million
Live and pilot users[4]	2,278
Services using InterAct[3]	68

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

InterAct traffic evolution

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



[5] growth rates 2016 and 2015 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.

Executive team and Board

Our executive team

Gottfried Leibbrandt
Chief Executive Officer

Gottfried Leibbrandt was appointed Chief Executive Officer in 2012. He joined SWIFT in 2005 to develop the *SWIFT2010* strategy, after which he was appointed Head of Standards and then promoted to Head of Marketing in 2007. As Head of Marketing Gottfried led the development and delivery of SWIFT's strategic initiatives and was a key architect behind the company's successful *SWIFT2015* strategy. Prior to joining SWIFT, Gottfried worked for McKinsey & Company as a co-leader of the European payments practice.

Marcel Bronmans
Chief Operations Officer

Marcel Bronmans was appointed 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, Marcel held positions as Chief Risk Officer and Head of Human Resources.

Javier Pérez-Tasso
Chief Executive Americas & UK Region

Javier Pérez-Tasso is Chief Executive of the Americas, the UK, Ireland and the 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, while earlier in his career, Javier held several senior leadership positions in SWIFT's sales and marketing divisions.

Alain Raes
Chief Executive, Asia Pacific and EMEA

Alain Raes was appointed Head 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.

Christian Sarafidis
Chief Marketing Officer

Christian Sarafidis was appointed Chief Marketing Officer in September 2015. He was previously Head of Western Europe, Middle East and Africa and Deputy Chief Executive, EMEA. Prior to joining SWIFT, Christian held senior executive positions for several multinational finance and technology groups.

Francis Vanbever
Chief Financial Officer

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

Craig Young
Chief Technology Officer

Craig Young took up his position as Chief Technology Officer in February 2015. He joined SWIFT from Verizon Communications, where he had worked for twenty 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.

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

Our Board of Directors

Yawar Shah
Chairman of the Board of Directors, SWIFT
Managing Director, Citi, USA
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

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

Claudio Camozzo
Co-Head of Global Transaction Banking (GTB), UniCredit, Italy
SWIFT Director since 2014

Fabrice Denèle
Head of Payments Group, BPCE, 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 Payments Market Infrastructure in Banking Group Treasury, FirstRand, South Africa
SWIFT Director since 2009
Chairman of the Audit & Finance Committee, SWIFT

Frederic Hannequart
Chief Business Development Officer, Euroclear, Belgium
SWIFT Director since 2014

Søren Haugaard
Global Head of Trade and Supply Chain Finance, Danske Bank, Denmark
SWIFT Director since 2015

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

Emma Loftus
Managing Director, Head of Global Payments, FX and Channels, 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

Kyoichi Nagata
Director, Transaction Services Division, The Bank of Tokyo-Mitsubishi UFJ, Japan
SWIFT Director since 2016

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

Javier Santamaria
Head of Payment Systems & Forums, Senior Vice President, Banco Santander, Spain
SWIFT Director since 2009

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 and Member of the Management Committee of KBC Bank and Insurance Belgium, Belgium
SWIFT Director since 2015

Qingsong Zhang
General Manager, Bank of China, Head Office Clearing Department, China
SWIFT Director since 2014

During the course of 2016 the following Directors left the Board:
Alan Goldstein, J.P. Morgan, USA
Yumesaku Ishigaki, The Bank of Tokyo-Mitsubishi UFJ, Japan
Marcus Treacher, HSBC, United Kingdom
Qingsong Zhang, Bank of China, China

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 10.

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 3.

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 & 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 2016 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 2016 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 CMPI-IOSCO'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.

SWIFT oversight

International cooperative oversight

Effective controls and processes

Open and constructive dialogue

Reviewing operational risk

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

The oversight objectives centre on: risk identification and management, information security, reliability and resilience, technology planning, and communication with users. 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, 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 report on Financial Market Infrastructures and Payment Services published by the National Bank of Belgium and is available on its website www.nbb.be.

Security audit and financial performance

2016 Security audit statement

The Directors and Management acknowledge their responsibility for maintaining an effective system of internal control in respect of the SWIFTNet and FIN services. SWIFT has put in place controls based on CPMI-IOSCO's Expectations for Critical Service Providers, to help achieve its control objectives in the areas of risk management, security management, technology management, resilience and user communication.

Management is satisfied that, for the period 1 January 2016 to 31 December 2016, the control policies and procedures relating to the SWIFTNet and FIN services were operating with sufficient effectiveness to provide reasonable assurance that appropriate governance was in place and the confidentiality, integrity, availability and change management objectives were met. The control objectives were specified by SWIFT Management.

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 specified by SWIFT Management covering the period of 1 January to 31 December 2016.

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 core messaging services.

Financial performance

In accordance with article 105 of the Belgian Code of Company Law, the following statements represent a condensed version of SWIFT's 2016 Consolidated Financial Statements prepared in accordance with International Financial Reporting Standards as adopted by the European Union. This condensed version does not contain all of the appendices or the report of the auditors, who expressed an unqualified opinion. The full text is available to SWIFT users on www.swift.com. The full version of the 2016 Consolidated Financial Statements will be filed with the National Bank of Belgium no later than 30 June 2017.

Key figures

For the year ended 31 December 2016

(in millions)	2016 EUR	2015 EUR	2014 EUR	2013 EUR	2012 EUR
Operating revenue before rebate	**745**	710	628	618	597
Rebate	**-**	(33)	(31)	(34)	-
Revenue after rebate	**745**	677	597	584	597
Operating expenses	**(691)**	(653)	(559)	(546)	(579)
Profit before taxation	**47**	35	38	35	21
Net profit	**26**	19	29	21	15
Net cash flow from operating activities	**53**	64	104	77	95
Capital expenditure of which:	**51**	48	38	46	70
property, plant and equipment	**42**	38	29	40	66
intangibles	**9**	10	9	6	4
Shareholders' equity	**415**	388	326	325	247
Total assets	**797**	763	714	603	603
Number of employees at end of year	**2,629**	2,328	2,163	2,010	1,928

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

Consolidated statement of profit and loss

For the year ended 31 December 2016

(in thousands)	Note	2016 EUR	2015 EUR restated*
Revenue			
Traffic revenue	2	**347,235**	298,802
One-time revenue	3	**19,896**	15,731
Recurring revenue	4	**208,576**	191,717
Interface revenue	5	**167,088**	157,695
Other operating revenue	6	**2,341**	12,653
		745,136	676,598
Expenses			
Royalties and cost of inventory	13	**(6,001)**	(8,053)
Payroll and related charges	7	**(352,982)**	(333,140)
Network expenses	8	**(13,840)**	(12,951)
External services expenses	9	**(263,765)**	(226,763)
Depreciation of property, plant and equipment	14	**(43,450)**	(39,301)
Amortisation of intangible assets	15	**(9,099)**	(7,491)
Other expenses	10	**(2,356)**	(25,639)
		(691,493)	(653,338)
Profit from operating activities		**53,643**	23,260
Financing costs	11	**(1,293)**	(1,358)
Other financial income and expenses	11	**(5,445)**	12,707
Profit before tax		**46,905**	34,609
Income tax expense	12	**(20,686)**	(15,111)
Net profit		**26,219**	**19,498**
Attributable to :			
Equity holders of the parent		**27,924**	21,616
Non-controlling interests	16	**(1,705)**	(2,118)
		26,219	19,498

* Certain amounts shown here do not correspond to the 2015 financial statements and reflect adjustments made, refer to Note 1.3.

Consolidated statement of comprehensive income

For the year ended 31 December 2016

			2016 EUR			2015 EUR		
(in thousands)		Note	Before tax	Tax (expense) benefit	Net of tax	Before tax	Tax (expense) benefit	Net of tax
Profit for the year	**(A)**		**46,905**	**(20,686)**	**26,219**	34,609	(15,111)	19,498
OCI items that may be reclassified subsequently to profit or loss:								
Foreign currency translation			**(87)**	**–**	**(87)**	(96)	-	(96)
Cash flow hedges:								
Current year gain/(loss) on financial instruments		31	**1,469**	**(500)**	**969**	(449)	152	(297)
Prior year (gain)/loss transferred to income statement		31	**449**	**(152)**	**297**	(3,611)	1,240	(2,371)
OCI items that will not be reclassified to profit or loss:								
Recognition of actuarial gains and losses		24	**(1,299)**	**(1,624)**	**(2,923)**	68,005	(22,225)	45,780
Other comprehensive income	**(B)**		**532**	**(2,276)**	**(1,744)**	63,849	(20,833)	43,016
Total comprehensive income for the year	**(A) + (B)**		**47,437**	**(22,962)**	**24,475**	**98,458**	**(35,944)**	**62,514**
Attributable to:								
Equity holders of the parent					**26,046**			64,292
Non-controlling interests					**(1,571)**			(1,778)
					24,475			62,514

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

Consolidated statement of financial position

For the year ended 31 December 2016

(in thousands)	Note	2016 EUR	2015 EUR restated*
Non-current assets			
Property, plant and equipment	14	**186,890**	189,212
Intangible assets	15	**20,947**	21,498
Deferred income tax assets	17	**74,392**	80,893
Other long-term assets	21	**15,739**	8,139
Total non-current assets		**297,968**	299,742
Current assets			
Cash and cash equivalents	18	**219,049**	212,538
Other current financial assets	18	**132,000**	132,591
Trade receivables	19	**75,236**	49,608
Other receivables	20	**22,432**	19,198
Prepayments to suppliers and accrued income	21	**44,223**	42,029
Inventories	22	**2,245**	2,750
Prepaid taxes	23	**3,987**	4,263
Total current assets		**499,172**	462,977
Total assets		**797,140**	762,719
Shareholders' equity		**415,332**	387,876
Equity attributable to equity holders of the parent		**409,519**	384,494
Non-controlling interests	16	**5,813**	3,382
Non-current liabilities			
Long-term employee benefits	24	**160,895**	153,806
Deferred income tax liabilities	17	**5,913**	7,740
Long-term provisions	26	**11,594**	22,461
Other long-term liabilities	27	**471**	834
Total non-current liabilities		**178,873**	184,841
Current liabilities			
Amounts payable to suppliers	31	**56,425**	61,065
Short-term employee benefits	25	**64,154**	61,902
Short-term provisions	26	**10,994**	8,937
Other liabilities	27	**65,040**	54,626
Accrued taxes	28	**6,322**	3,472
Total current liabilities		**202,935**	190,002
Total equity and liabilities		**797,140**	762,719

* Certain amounts shown here do not correspond to the 2015 financial statements and reflect adjustments made, refer to Note 1.3.

Consolidated statement of cash flows

For the year ended 31 December 2016

(in thousands)	Note	2016 EUR	2015 EUR
Cash flow from operating activities			
Profit before taxation		**46,905**	34,609
Depreciation of property, plant and equipment	14	**43,450**	39,301
Amortisation of intangible assets	15	**9,099**	7,491
Net (gain)/loss and write-off on sale of property, plant and equipment, and intangible assets		**70**	(10,320)
Other non-cash operating losses/(gains)			
Increase/(decrease) in provisions, pensions and government grants		**(711)**	32,976
(Increase)/decrease in other net long-term assets		**(7,963)**	2,588
Net financial (income)/costs		**1,829**	1,337
Net unrealised exchange (gain)/loss		**(707)**	(5,527)
Increase/(decrease) in other non-cash operating items		**3,096**	(236)
Changes in net working capital			
(Increase)/decrease in trade and other receivables and prepayments		**(31,056)**	4,575
(Increase)/decrease in inventories	22	**505**	3,570
Increase/(decrease) in trade and other payables		**5,775**	18,352
Investments in other financial assets	18	**591**	(35,522)
Net cash flow before interest and tax		**70,883**	93,194
Interest received		**671**	767
Interest paid		**(2,483)**	(2,100)
Tax paid		**(15,773)**	(27,436)
Net cash flow from operating activities		**53,298**	64,425
Cash flow from investing activities			
Capital expenditures			
Property, plant and equipment	14	**(42,074)**	(38,491)
Intangibles	15	**(8,558)**	(9,509)
Proceeds from sale of fixed assets		**886**	19,531
Capital increase in partly-owned subsidiaries		**4,002**	-
Net cash flow used in investing activities		**(45,744)**	(28,469)
Cash flow from financing activities			
Net payments for reimbursement of capital		**(474)**	(320)
Net cash flow from (used in) financing activities		**(474)**	(320)
Increase/(decrease) of cash and cash equivalents		**7,080**	35,636
Movement in cash and cash equivalents			
At the beginning of the year		**212,538**	174,188
Increase/(decrease) of cash and cash equivalents		**7,080**	35,636
Effects of exchange rate changes		**(569)**	2,714
At the end of the year	18	**219,049**	212,538
Cash and cash equivalent components are:			
Cash	18	**25,517**	85,134
Liquid money market products	18	**193,532**	127,404
At the end of the year	18	**219,049**	212,538

SWIFT offices

Global presence

27 offices worldwide

Connecting more than 200 countries and territories

Americas

Brazil
Rua Iaia, 77 Cj. 52
Itaim Bibi
04542-060 São Paulo – SP
Tel: +55 11 3514 9004

Mexico
Col. Juarez
Paseo de la Reforma # 350, 11th floor
Mexico City, 06600
Tel +52 55 2881 6742

United States – Miami
600 Brickell Avenue, suite 1800
Miami, FL 33131
Tel: +1 305 913 7184

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

Asia Pacific

Australia
AMP Centre, level 36, suite 3603
50, Bridge Street
Sydney, NSW 2000
Tel: +61 2 92 25 8100

China – Beijing
Winland International Finance Centre,
units 902-903, 9th floor
7, Financial Street
Xicheng District
Beijing 100033
Tel: +86 10 6658 2900

China – Hong Kong
One Island East, suites 3201-09,
32nd floor
18, Westlands Road
One Island East, Hong Kong
Tel: +852 2107 8700

China – Shanghai
Two IFC, unit 4606-08, level 46
8, Century Avenue
Pudong, Shanghai
Tel: +86 21 8021 8000

India
The Capital, plot C-70, G Block, unit
no.1303, 13th floor
G Block, Bandra-Kurla Complex,
Bandra (East)
Mumbai 400 051
Tel: +91 22 6196 6900

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

Korea
Korea First Bank Building, 20th floor
100 Gongpyung-dong, Chungno-gu
Seoul
Tel: +82 2 2076 8236

Malaysia
The Horizon, level 18, tower 3, avenue 7
Bangsar South
8, Jalan Kerinchi
59200 Kuala Lumpur
Tel: +603 2773 7500

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

Europe, Middle East and Africa

Austria
BENA City Centre
Fischhof 3
A-1010 Vienna
Tel: +43 1 74040 2372

Belgium
Global Headquarters
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
City-Haus I
Platz der Republik 6
D-60325 Frankfurt am Main
Tel: +49 69 7541 2200

Ghana
Presidential Floor
Mövenpick Ambassador Hotel Accra
Independence Avenue Ridge
Accra
Tel: +234 1 4489204

Italy
6th Floor, Corso G. Matteotti 10
20121 Milano
Tel: +39 02 7742 5000

Kenya
Delta Corner, 7th floor, office 712
Westlands
00800 Nairobi
Tel: +254 7 3011 2000

Russian Federation
LOTTE Business Centre, 9th floor
8, Novinsky Boulevard
121099 Moscow
Tel: +7 495 228 5923

South Africa
1, Melrose Boulevard, unit 18, 2nd floor
Melrose Arch
Gauteng, 2076
Tel: +27 11 218 5353

Spain
Edificio Cuzco IV
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
The Corn Exchange, 6th floor
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 on www.swift.com.

To view this annual review online, please visit:
www.swift.com

57268 – May 2017

FSC
www.fsc.org
MIX
Paper from
responsible sources
FSC® C016486

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.