Society for Worldwide Interbank Financial Telecommunication

From Wikipedia, the free encyclopedia

The **Society for Worldwide Interbank Financial Telecommunication** (**SWIFT**) provides a network that enables financial institutions worldwide to send and receive information about financial transactions in a secure, standardized and reliable environment. SWIFT also sells software and services to financial institutions, much of it for use on the SWIFTNet Network, and ISO 9362. Business Identifier Codes (BICs, previously Bank Identifier Codes) are popularly known as "SWIFT codes".

Society for Worldwide Interbank Financial Telecommunication

Type	Cooperative
Industry	Telecommunications
Founded	1973
Headquarters	La Hulpe, Belgium
Key people	Yawar Shah (Chairman); Gottfried Leibbrandt (CEO)
Products	Financial Telecommunication
Number of employees	>2000
Website	www.swift.com (http://www.swift.com)

The majority of international interbank messages use the SWIFT network. As of 2015, SWIFT linked more than 11,000 financial institutions in more than 200 countries and territories, who were exchanging an average of over 15 million messages per day (compared to an average of 2.4 million daily messages in 1995).[1] SWIFT transports financial messages in a highly secure way but does not hold accounts for its members and does not perform any form of clearing or settlement.

SWIFT does not facilitate funds transfer: rather, it sends payment orders, which must be settled by correspondent accounts that the institutions have with each other. Each financial institution, to exchange banking transactions, must have a banking relationship by either being a bank or affiliating itself with one (or more) so as to enjoy those particular business features.

SWIFT is a cooperative society under Belgian law owned by its member financial institutions with offices around the world. SWIFT headquarters, designed by Ricardo Bofill Taller de Arquitectura are in La Hulpe, Belgium, near Brussels. The chairman of SWIFT is Yawar Shah,[2] originally from Pakistan,[3] and its CEO is Gottfried Leibbrandt, originally from the Netherlands.[4] SWIFT hosts an annual conference every year, called Sibos, specifically aimed at the financial services industry.

Contents

History

SWIFT was founded in Brussels in 1973 under the leadership of its inaugural CEO Carl Reuterskiöld (1973–1983) and was supported by 239 banks in fifteen countries. It started to establish common standards for financial transactions and a shared data processing system and worldwide communications network designed by Logica.[5] Fundamental operating procedures, rules for liability, etc., were established in 1975 and the first message was sent in 1977. SWIFT's first United States operating center was inaugurated by Governor John N. Dalton of Virginia in 1979.[6]

Standards

SWIFT has become the industry standard for syntax in financial messages. Messages formatted to SWIFT standards can be read by, and processed by, many well-known financial processing systems, whether or not the message traveled over the SWIFT

network. SWIFT cooperates with international organizations for defining standards for message format and content. SWIFT is also *Registration authority* (RA) for the following ISO standards: [7]

- ISO 9362: 1994 Banking—Banking telecommunication messages—Bank identifier codes
- ISO 10383: 2003 Securities and related financial instruments—Codes for exchanges and market identification (MIC)
- ISO 13616: 2003 IBAN Registry
- ISO 15022: 1999 Securities—Scheme for messages (Data Field Dictionary) (replaces ISO 7775)
- ISO 20022-1: 2004 and ISO 20022-2:2007 Financial services—Universal Financial Industry message scheme

In RFC 3615 *urn:swift:* was defined as Uniform Resource Names (URNs) for SWIFT FIN.[8]

Operations centers

The SWIFT secure messaging network is run from two redundant data centers, one in the United States and one in the Netherlands. These centers share information in near real-time. In case of a failure in one of the data centers, the other is able to handle the traffic of the complete network.

SWIFT opened a third data center in Switzerland, which started operating in 2009.[9] Since then, data from European SWIFT members are no longer mirrored to the U.S. data center. The distributed architecture partitions messaging into two messaging zones: European and Trans-Atlantic.[10] European zone messages are stored in the Netherlands and in a part of the Switzerland operating center; Trans-Atlantic zone messages are stored in the United States and in a part of the Switzerland operating center that is segregated from the European zone messages. Countries outside of Europe were by default allocated to the Trans-Atlantic zone but could choose to have their messages stored in the European zone.

SWIFTNet network

SWIFT moved to its current IP network infrastructure, known as SWIFTNet, from 2001 to 2005,[11] providing a total replacement of the previous X.25 infrastructure. The process involved the development of new protocols that facilitate efficient messaging, using existing and new message standards. The adopted technology chosen to develop the protocols was XML, where it now provides a wrapper around all messages legacy or contemporary. The communication protocols can be broken down into:

InterAct

- SWIFTNet InterAct Realtime
- SWIFTNet InterAct Store and Forward

FileAct

- SWIFTNet FileAct Realtime
- SWIFTNet FileAct Store and Forward

Browse

- SWIFTNet Browse

Architecture

SWIFT provides a centralized store-and-forward mechanism, with some transaction management. For bank A to send a message to bank B with a copy or authorization with institution C, it formats the message according to standard and securely sends it to SWIFT. SWIFT guarantees its secure and reliable delivery to B after the appropriate action by C. SWIFT guarantees are based primarily on high redundancy of hardware, software, and people.

SWIFTNet Phase 2

During 2007 and 2008, the entire SWIFT Network migrated its infrastructure to a new protocol called SWIFTNet Phase 2. The main difference between Phase 2 and the former arrangement is that Phase 2 requires banks connecting to the network to use a Relationship Management Application (RMA) instead of the former bilateral key exchange (BKE) system. According to SWIFT's public information database on the subject, RMA software should eventually prove more secure and easier to keep up-to-date; however, converting to the RMA system meant that thousands of banks around the world had to update their international payments systems to comply with the new standards. RMA completely replaced BKE on 1 January 2009.

Products and interfaces

SWIFT means several things in the financial world:

1. a secure network for transmitting messages between financial institutions;
2. a set of syntax standards for financial messages (for transmission over SWIFTNet or any other network)
3. a set of connection software and services allowing financial institutions to transmit messages over SWIFT network.

Under 3 above, SWIFT provides turn-key solutions for members, consisting of linkage clients to facilitate connectivity to the SWIFT network and CBTs or 'computer based terminals' which members use to manage the delivery and receipt of their messages.

Some of the more well-known interfaces and CBTs provided to their members are:

- SWIFTNet Link (SNL) software which is installed on the SWIFT customer's site and opens a connection to SWIFTNet. Other applications can only communicate with SWIFTNet through the SNL.
- Alliance Gateway (SAG) software with interfaces (e.g., RAHA = Remote Access Host Adapter), allowing other software products to use the SNL to connect to SWIFTNet
- Alliance WebStation (SAB) desktop interface for SWIFT Alliance Gateway with several usage options:

1. administrative access to the SAG
2. direct connection SWIFTNet by the SAG, to administrate SWIFT Certificates
3. so-called Browse connection to SWIFTNet (also by SAG) to use additional services, for example Target2

- Alliance Access (SAA) and Alliance Messaging Hub (AMH) are the main messaging software applications by SWIFT, which allow message creation for FIN messages, routing and monitoring for FIN and MX messages. The main interfaces are FTA (files transfer automated, not FTP) and MQSA, a WebSphere MQ interface.
- The Alliance Workstation (SAW) is the desktop software for administration, monitoring and FIN message creation. Since Alliance Access is not yet capable of creating MX messages, Alliance Messenger (SAM) has to be used for this purpose.
- Alliance Web Platform (SWP) as new thin-client desktop interface provided as an alternative to existing Alliance WebStation, Alliance Workstation (soon) and Alliance Messenger.
- Alliance Integrator built on Oracle's Java Caps which enables customer's back office applications to connect to Alliance Access or Alliance Entry.
- Alliance Lite2 is a secure and reliable, cloud-based way to connect to the SWIFT network which is a Lite version of Alliance Access specifically targeting customers with low volume of traffic.

Services

There are four key areas that SWIFT services fall under in the financial marketplace: Securities, Treasury & Derivatives, Trade Services and Payments & Cash Management.

Securities	**Treasury & Derivatives**	**Cash Management**	**Trade Services**
▪ SWIFTNet FIX (obsolete) ▪ SWIFTNet Data Distribution	▪ SWIFTNet Accord for Treasury (*end of*	▪ SWIFTNet Bulk Payments ▪ SWIFTNet Cash Reporting	▪ SWIFTNet Trade Services Utility

- SWIFTNet Funds
- SWIFTNet Accord for Securities (*end of life October 2017*)[12]
- SWIFTNet Affirmations
- SWIFTNet CLS Third Party Service
- SWIFTNet Exceptions and Investigations

SWIFTREF

Swift Ref, the global payment reference data utility, is SWIFT's unique reference data service. Swift Ref sources data direct from data originators, including central banks, code issuers and banks making it easy for issuers and originators to maintain data regularly and thoroughly. SWIFTRef constantly validates and cross-checks data across the different data sets.[13]

SWIFTNet Mail

SWIFT offers a secure person-to-person messaging service, SWIFTNet Mail, which went live on 16 May 2007.[14] SWIFT clients can configure their existing email infrastructure to pass email messages through the highly secure and reliable SWIFTNet network instead of the open Internet. SWIFTNet Mail is intended for the secure transfer of sensitive business documents, such as invoices, contracts and signatories, and is designed to replace existing telex and courier services, as well as the transmission of security-sensitive data over the open Internet. Seven financial institutions, including HSBC, FirstRand Bank, Clearstream, DnB NOR, Nedbank, and Standard Bank of South Africa, as well as SWIFT piloted the service.[15]

U.S. government involvement

Terrorist Finance Tracking Program

A series of articles published on 23 June 2006 in *The New York Times*, *The Wall Street Journal*, and the *Los Angeles Times* revealed a program, named the Terrorist Finance Tracking Program, which the US Treasury Department, Central Intelligence Agency (CIA), and other United States governmental agencies initiated after the 11 September attacks to gain access to the SWIFT transaction database.[16]

After the publication of these articles, SWIFT quickly came under pressure for compromising the data privacy of its customers by allowing governments to gain access to sensitive personal information. In September 2006, the Belgian government declared

that these SWIFT dealings with American governmental authorities were a breach of Belgian and European privacy laws.

In response, and to satisfy members' concerns about privacy, SWIFT began a process of improving its architecture by implementing a distributed architecture with a two-zone model for storing messages (see Operations centers).

Concurrently, the European Union negotiated an agreement with the United States Government to permit the transfer of intra-EU SWIFT transaction information to the United States under certain circumstances. Because of concerns about its potential contents, the European Parliament adopted a position statement in September 2009, demanding to see the full text of the agreement and asking that it be fully compliant with EU privacy legislation, with oversight mechanisms emplaced to ensure that all data requests were handled appropriately.[17] An interim agreement was signed without European Parliamentary approval by the European Council on 30 November 2009,[18] the day before the Lisbon Treaty—which would have prohibited such an agreement from being signed under the terms of the Codecision procedure—formally came into effect. While the interim agreement was scheduled to come into effect on 1 January 2010, the text of the agreement was classified as "EU Restricted" until translations could be provided in all EU languages and published on 25 January 2010.

On 11 February 2010, the European Parliament decided to reject the interim agreement between the EU and the USA with 378 to 196 votes.[19][20] One week earlier, the parliament's civil liberties committee already rejected the deal, citing legal reservations.[21]

In March 2011, it was reported that two mechanisms of data protection had failed: EUROPOL released a report complaining that the USA's requests for information had been too vague (making it impossible to make judgments on validity)[22] and that the guaranteed right for European citizens to know whether their information had been accessed by USA authorities had not been put into practice.[22]

Sanctions against Iran

In January 2012, the advocacy group United Against Nuclear Iran (UANI) implemented a campaign calling on SWIFT to end all relations with Iran's banking system, including the Central Bank of Iran. UANI asserted that Iran's membership in SWIFT violated U.S. and EU financial sanctions against Iran as well as SWIFT's own corporate rules.[23]

Consequently, in February 2012, the U.S. Senate Banking Committee unanimously approved sanctions against SWIFT aimed at pressuring the Belgian financial telecommunications network to terminate its ties with blacklisted Iranian banks.

Expelling Iranian banks from SWIFT would potentially deny Iran access to billions of dollars in revenue and spending using SWIFT but not from using IVTS. Mark Wallace, president of UANI, praised the Senate Banking Committee.[24]

Initially SWIFT denied it was acting illegally,[24] but now says "it is working with U.S. and European governments to address their concerns that its financial services are being used by Iran to avoid sanctions and conduct illicit business."[25] Targeted banks would be — amongst others — Saderat Bank of Iran, Bank Mellat, Post Bank of Iran and Sepah Bank.[26] On 17 March 2012, following agreement two days earlier between all 27 member states of the Council of the European Union and the Council's subsequent ruling, SWIFT disconnected all Iranian banks from its international network that had been identified as institutions in breach of current EU sanctions and warned that even more Iranian financial institutions could be disconnected from the network.

In February 2016, Iranian banks reconnected to the network following lift of sanctions on Joint Comprehensive Plan of Action.[27]

U.S. control over transactions within the EU

On 26 February 2012 the Danish newspaper *Berlingske* reported that US authorities have sufficient control over SWIFT to seize money being transferred between two European Union (EU) countries (Denmark and Germany), since they have seized around US$26,000 which was being transferred from a Danish businessman to a German bank. The transaction was automatically routed through the US, possibly because of the USD currency used in the transaction which is how the United States was able to seize the funds. The money was a payment for a batch of Cuban cigars previously imported to Germany by a German supplier. As justification for the seizure, the U.S. Treasury stated that the Danish businessman had violated the United States embargo against Cuba.[28][29]

Monitoring by the NSA

Der Spiegel reported in September 2013 that the National Security Agency (NSA) widely monitors banking transactions via SWIFT, as well as credit card transactions.[30] The NSA intercepted and retained data from the SWIFT network used by thousands of banks to securely send transaction information. SWIFT was named as a "target", according to documents leaked by Edward Snowden. The documents revealed that the NSA spied on SWIFT using a variety of methods, including reading "SWIFT printer traffic from numerous banks."[30] In April 2017, a group known as the Shadow Brokers released files allegedly from the NSA which indicate that the agency monitored financial transactions made through SWIFT.[31][32]

Use in sanctions

As mentioned above SWIFT has disconnected all Iranian banks from its international network as a sanction against Iran. Similarly, in August 2014 the UK planned to press the EU to block Russian use of SWIFT as a sanction due to Russian military intervention in Ukraine.[33] However, SWIFT refused to do so. In their official statement they said, "SWIFT regrets the pressure, as well as the surrounding media speculation, both of which risk undermining the systemic character of the services that SWIFT provides its customers around the world".[34] SWIFT also rejected calls to boycott Israeli banks from its network.[35]

Security

In 2016 an $81 million theft from the Bangladesh central bank via its account at the New York Federal Reserve Bank was traced to hacker penetration of SWIFT's Alliance Access software, according to a New York *Times* report. It was not the first such attempt, the society acknowledged, and the security of the transfer system was undergoing new examination accordingly.[36] Soon after the reports of the theft from the Bangladesh central bank, a second, apparently related, attack was reported to have occurred on a commercial bank in Vietnam.[37][38]

Both attacks involved malware written to both issue unauthorized SWIFT messages and to conceal that the messages had been sent. After the malware sent the SWIFT messages that stole the funds, it deleted the database record of the transfers then took further steps to prevent confirmation messages from revealing the theft. In the Bangladeshi case, the confirmation messages would have appeared on a paper report; the malware altered the paper reports when they were sent to the printer. In the second case, the bank used a PDF report; the malware altered the PDF viewer to hide the transfers.[37]

In May 2016, Banco del Austro (BDA) in Ecuador sued Wells Fargo after Wells Fargo honored $12 million in fund transfer requests that had been placed by thieves.[38] In this case, the thieves sent SWIFT messages that resembled recently canceled transfer requests from BDA, with slightly altered amounts; the reports do not detail how the thieves gained access to send the SWIFT messages. BDA asserts that Wells Fargo should have detected the suspicious SWIFT messages, which were placed outside of normal BDA working hours and were of an unusual size. Wells Fargo claims that BDA is responsible for the loss, as the thieves gained access to the legitimate SWIFT credentials of a BDA employee and sent fully authenticated SWIFT messages.[38]

In the first half of 2016, an anonymous Ukrainian bank, with the episode being investigated by ISACA, and others -- even "dozens" that are not being made public -- were variously reported to have been "compromised" through the SWIFT network and to have lost money.[39]

See also

- Bilateral key exchange and the new Relationship Management Application (RMA)
- Electronic money
- ISO 9362, the SWIFT/BIC code standard
- ISO 15022
- ISO 20022
- Organization for Economic Cooperation and Development (OECD)
- Routing transit number
- Sibos conference
- Terrorist Finance Tracking Program
- TIPANET
- Value transfer system

References

1. "Swift Company Information" (http://www.swift.com/about_swift/company_information/index.page?lang=en). SWIFT. 9 March 2010. Retrieved 7 December 2016.
2. "Board members" (https://www.swift.com/about-us/organisation-governance/board-members#topic-tabs-menu). *SWIFT*. 9 December 2015. Retrieved May 4, 2016.
3. "Yawar Shah - 1996 - 40 Under Forty - Crain's New York Business" (http://mycrains.crainsnewyork.com/40under40/profiles/1996/yawar-shah). Retrieved 2014-02-23.
4. "SWIFT Management" (https://www.swift.com/about-us/organisation-governance/swift-management#topic-tabs-menu). *SWIFT*. 7 October 2015. Retrieved May 4, 2016.
5. "Logica history" (http://www.logica.com/we-are-logica/about-logica/history-and-key-milestones/).
6. "Carl Reuterskiöld" (http://www.swift.com/about_swift/press_room/swift_news_archive/home_page_stories_archive_2006/61159/carl_reuterski_ld.page?). SWIFT. March 2006. Retrieved 7 September 2012.
7. "ISO Maintenance agencies and registration authorities]" (http://www.iso.org/iso/standards_development/maintenance_agencies.htm).
8. "RFC 3615 – A Uniform Resource Name (URN) Namespace for SWIFT Fin" (http://www.faqs.org/rfcs/rfc3615.html).
9. "SWIFT: SIBOS issues" (http://www.swift.com/sibos2008/sibos_2008_learn_discuss_debate/sibos_issues/Sibos_Issues_20080916.pdf) (PDF). SWIFT. 16 September 2008. p.12
10. "Distributed architecture" (http://www.swift.com/products_services/industry_initiatives/distributed_architecture). SWIFT. 6 June 2008.
11. "SWIFT History" (http://www.swift.com/about_swift/company_information/swift_history.page?lang=en). SWIFT.
12. "Accord" (https://www.swift.com/our-solutions/a-to-z/accord). 26 November 2015.
13. "SWIFTREF" (http://www.surecomp.com/value-added.html).
14. "SWIFTNet Mail now available" (http://www.swift.com/about_swift/press_room/press_releases/press_releases_archive/mail_simple_secure_and_reliable_email.page).

15. "SWIFTNet Mail pilot phase underway" (http://www.swift.com/index.cfm?item_id=61132).
16. Brand, Constant (28 September 2005). "Belgian PM: Data Transfer Broke Rules" (http://www.washingtonpost.com/wp-dyn/content/article/2006/09/28/AR2006092800585.html). Washington Post. Retrieved 23 May 2010.
17. "European Parliament resolution of 17 September 2009 on the SWIFT Agreement" (http://www.europarl.europa.eu/sides/getDoc.do?type=TA&reference=P7-TA-2009-0016&language=EN&ring=B7-2009-0038). European Parliament. 17 September 2009.
18. "European Parliament to vote on interim agreement at February session" (http://www.europarl.europa.eu/news/expert/infopress_page/019-67614-018-01-04-902-20100119IPR67613-18-01-2010-2010-false/default_en.htm). European Parliament. 21 January 2010.
19. Brand, Constant (11 February 2010), "Parliament rejects bank transfer data deal" (http://www.europeanvoice.com/article/2010/02/parliament-rejects-bank-transfer-data-deal/67144.aspx), *European Voice*
20. "Euro MPs block bank data deal with US" (http://news.bbc.co.uk/2/hi/europe/8510471.stm), *BBC News*, 11 February 2010
21. "European parliament rejects SWIFT deal for sharing bank data with US" (http://www.dw.com/en/european-parliament-rejects-swift-deal-for-sharing-bank-data-with-us/a-5239595), *Reuters via DW*, 11 February 2010
22. Schult, Christoph (16 March 2011). "Brussels Eyes a Halt to SWIFT Data Agreement" (http://www.spiegel.de/international/europe/0,1518,751262,00.html). *Der Spiegel*.
23. Gladstone, Rick (31 January 2012). "Iran Praises Nuclear Talks With Team From U.N." (https://www.nytimes.com/2012/02/01/world/middleeast/iran-calls-un-nuclear-teams-visit-constructive.html?_r=1). *The New York Times*. Retrieved 4 February 2012.
24. Gladstone, Rick (3 February 2012). "Senate Panel Approves Potentially Toughest Penalty Yet Against Iran's Wallet" (https://www.nytimes.com/2012/02/03/world/middleeast/tough-iran-penalty-clears-senate-banking-panel.html?_r=2&ref=world). *The New York Times*. Retrieved 4 February 2012.
25. Solomon, Jay; & Adam Entous (4 February 2012). "Banking Hub Adds to Pressure on Iran" (https://www.wsj.com/articles/SB10001424052970203889904577201330206741436?mod=googlenews_wsj). *The Wall Street Journal*. Retrieved 4 February 2012.
26. "Banking's SWIFT says ready to block Iran transactions" (https://www.reuters.com/article/2012/02/17/iran-sanctions-swift-idUSL5E8DH31020120217). 17 February 2012. Retrieved 17 February 2012.
27. Torchia, Andrew (17 February 2016). "Iranian banks reconnected to SWIFT network after four-year hiatus" (https://www.reuters.com/article/us-iran-banks-swift-idUSKCN0VQ1FD). Reuters. Retrieved 21 April 2016.
28. Bendtsen, Simon; Benson, Peter Suppli (26 February 2012). "Dansk politimand fanget i amerikansk terrornet" (http://www.b.dk/nationalt/dansk-politimand-fanget-i-amerikansk-terrornet) [Danish policeman caught in American terror net]. *Berlingske* (in Danish). Retrieved 26 February 2012.
29. "US snubs out legal cigar transaction" (http://cphpost.dk/news14/international-news14/us-snubs-out-legal-cigar-transaction.html). *The Copenhagen Post*. 2012-02-27. Retrieved 2016-04-12.
30. " 'Follow the Money': NSA Spies on International Payments" (http://www.spiegel.de/international/world/spiegel-exclusive-nsa-spies-on-international-bank-transactions-a-922276.html). *SPIEGEL ONLINE International*. Der Speigel. 15 September 2013. Retrieved 18 September 2013.
31. Baldwin, Clare (15 April 2017). "Hackers release files indicating NSA monitored global bank transfers" (https://www.reuters.com/article/us-usa-cyber-swift-idUSKBN17G1HC). Reuters. Retrieved 15 April 2017.
32. Lawler, Richard. "Shadow Brokers release also suggests NSA spied on bank transactions" (https://www.engadget.com/2017/04/14/shadow-brokers-release-also-suggest-nsa-spied-on-bank-transactio/). *Engadget*. Retrieved 15 April 2017.

33. Hutton, Robert; Ian Wishart (29 August 2014). "U.K. Wants EU to Block Russia From SWIFT Banking Network" (https://www.bloomberg.com/news/2014-08-29/u-k-wants-eu-to-block-russia-from-swift-banking-network.html). *Bloomberg News*. Retrieved 31 August 2014.
34. "SWIFT Sanctions Statement" (http://www.swift.com/about_swift/shownews?param_dcr=news.data/en/swift_com/2014/PR_swift_sanctions_statement.xml). *swift.com*.
35. International banking giant refuses to cut off Israel, despite boycott calls (http://www.haaretz.com/business/.premium-1.619514). Haaretz. 7 October 2014.
36. Corkery, Michael, "Hackers' $81 Million Sneak Attack on World Banking" (https://www.nytimes.com/2016/05/01/business/dealbook/hackers-81-million-sneak-attack-on-world-banking.html), New York *Times*, April 30, 2016. Retrieved 2016-05-01.
37. Corkery, Michael (12 May 2016). "Once Again, Thieves Enter Swift Financial Network and Steal" (https://www.nytimes.com/2016/05/13/business/dealbook/swift-global-bank-network-attack.html). *New York Times*. Retrieved 13 May 2016.
38. Bergin, Tom; Layne, Nathan (20 May 2016). "Special Report: Cyber thieves exploit banks' faith in SWIFT transfer network" (https://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD). Reuters. Retrieved 24 May 2016.
39. Metzger, Max (June 28, 2016). "SWIFT robbers swoop on Ukrainian bank" (http://www.scmagazineuk.com/swift-robbers-swoop-on-ukrainian-bank/article/506140/). SC Magazine UK. Retrieved June 29, 2016.

External links

- Official website (http://www.swift.com)