Congressional Research Service
Informing the legislative debate since 1914

International Financial Messaging Systems

July 19, 2021

Congressional Research Service
https://crsreports.congress.gov
R46843

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R46843

July 19, 2021

Liana Wong
Analyst in International Trade and Finance

Rebecca M. Nelson
Specialist in International Trade and Finance

International Financial Messaging Systems

The growth of international trade in goods and services has led to a growth in the volume and value of cross-border payments. International financial messaging systems play an important role as part of the global financial infrastructure. These systems enable financial institutions to send and receive financial messages, carrying information about the transactions (e.g., sender, recipient, type of transaction, and amount) so financial institutions can verify the legitimacy of the transactions before they are settled and made available in the recipients' accounts. Financial messages are also used by financial institutions and regulators to enforce regulations issued to curtail money laundering and terrorist financing. The intersection of international financial messaging systems with U.S. sanctions, and the development of new financial messaging systems, may be of interest to Congress.

An international funds transfer typically involves the senders' and recipient's banks, a clearing settlement institution, and an electronic financial message containing instructions for the transfer. National payment systems, like the Federal Reserve's Fedwire System, have their own financial messaging networks and provide clearing and settlement services, but their services are limited to domestic financial institutions. The Society of Worldwide Interbank Financial Telecommunication (SWIFT) is currently the primary international financial messaging service for cross-border payments sent between financial institutions in different countries. It does not provide clearing and settlement services like national payment systems. Founded in 1973, SWIFT is a cooperative organization headquartered in Belgium, owned by over 2,400 financial institutions, and governed by an elected board of 25 directors. At least 11,500 financial institutions from 200 countries use SWIFT's messaging services for cross-border payments. In 2019, more than 8.4 billion financial messages were sent over the SWIFT network, compared to 3.8 billion in 2009. The daily average of messages sent within a year more than doubled between 2009 and 2019, from 14.9 million to 33.5 million.

While SWIFT's vast network connects financial institutions to each other around the world, policymakers and financial institutions have raised concerns about the speed, cost, and lack of transparency of its messaging services. A number of cyberattacks on financial institutions that resulted in the initiation of fraudulent transfers using SWIFT credentials have also raised questions regarding the security of the network and the cross-border payments system as a whole. In recent years, alternative financial messaging systems have been introduced as a solution to some of these concerns; these would replace SWIFT entirely. Financial technology companies and financial institutions in the private sector have created cross-border payments networks using blockchain technology, stating that it is cheaper, faster, and more transparent than the legacy system. Many central banks are also exploring the creation of their own digital currencies that could, depending on their design, reduce reliance on SWIFT.

China and Russia have created financial messaging systems of their own and have plans to link the two together, along with India's planned system to support cross-border payments in their own currencies. There have also been multilateral efforts to improve the cross-border payments process by improving existing infrastructure like SWIFT, encouraging international cooperation in harmonizing regulation and standards, and integrating emerging technology into existing services.

Policy issues have arisen between U.S. sanctions policies and international financial messaging systems. The United States government has increasingly relied on financial sanctions to advance its foreign policy objectives. Since SWIFT is incorporated in Belgium, U.S. sanctions do not prohibit SWIFT from processing financial messages to or from entities subject to sanctions by the U.S. government. In the case of Iran, Congress authorized sanctions against international financial messaging systems themselves unless they removed certain Iranian financial institutions from their systems. SWIFT ultimately removed the Iranian entities in question in order to avoid sanctions that could have been potentially destabilizing to the global economy.

Congress may consider a number of issues as new technology and financial service providers change the current cross-border payment landscape. What is the impact of new services on U.S. consumers and businesses, as well as U.S. economic, national security, and foreign policy objectives? As China and Russia create their own financial systems, should the United States create its own? Should the U.S. government promote more multilateral cooperation on cross-border payment issues like cost, transparency, anti-corruption, and cybersecurity? Should the U.S. government use sanctions against financial messaging systems like SWIFT to advance U.S. foreign policy goals and what are the potential impacts to the United States of such actions?

Contents

Introduction 1
What are Financial Messaging Systems? 1
Role in Cross-Border Financial Transactions 1
Society for Worldwide Interbank Financial Telecommunication 2
Concerns and Issues Regarding SWIFT 5
Changing Landscape for Cross-Border Financial Messages 7
Blockchain and Digital Currencies 8
China's Cross-Border Interbank Payment Systems 9
Russia's System for Transfer of Financial Messages 10
Instrument In Support of Trade Exchange 11
Cross-Border Payment Challenges and Multilateral Responses 11
Financial Messaging Systems and U.S. Sanctions 12
Financial Messages and U.S. Sanctions on Iran 13
Financial Messages and U.S. Sanctions on North Korea 14
Other Political Pressures on Financial Messaging Providers 15
Selected Policy Issues for Congress 16

Figures

Figure 1. Simple Cross-Border Payment Process 2
Figure 2. SWIFT at a Glance 4
Figure 3. Cross-border Interbank Payment Systems Participants 10
Figure 4. U.S. Sanctions on Iran and Financial Messages: Timeline 14

Contacts

Author Information 17

Introduction

The integration of international merchandise, services, and financial markets over the past several decades has increased the volume and value of cross-border payments. Processing a cross-border payment is more complicated than processing a domestic payment. Financial messaging systems play an important role in facilitating cross-border payments for international trade, investment, and remittances.

This report explains the role of financial messaging systems in the global financial infrastructure—often considered the backbone or "plumbing" of the global economy. It discusses recent trends, including efforts by some foreign governments to create their own financial messaging systems, and technological developments that may reduce the need for financial messaging systems. The report discusses congressional debate over the use of sanctions to induce international messaging systems to remove certain financial institutions from their systems, as part of a broader effort to advance U.S. foreign policy and national security goals. Finally, it presents a number of policy issues Congress may consider in shaping U.S. economic and foreign policy to promote global economic stability and efficient facilitation of cross-border payments.

What are Financial Messaging Systems?

Financial institutions use financial messaging systems to send and receive financial messages, which are then used by the institutions to confirm the payment type and amount, and the identities of the sender and recipient participating in a transaction. Financial messages are also used by financial institutions and regulators in the enforcement of financial regulations related to money laundering, terrorist financing, and know-your-customer checks.

Financial messages contain standardized codes that provide information and instructions for financial transactions. The International Organization for Standardization (ISO) develops and publishes standards for financial messages. ISO, founded in 1947 and located in Switzerland, is an international standards-setting body composed of representatives from various national standards organizations, including the American National Standards Institute from United States. Many financial institutions and payment systems use ISO standards for financial messages.[1]

Role in Cross-Border Financial Transactions

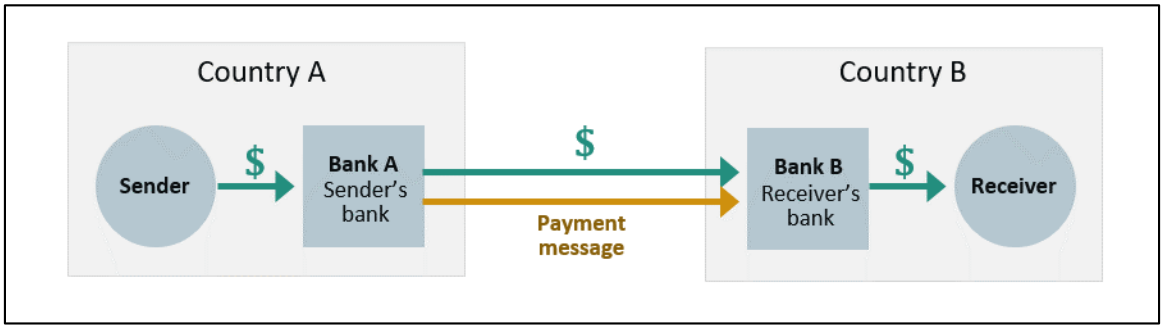
Typically, an international funds transfer involves the sender's and recipient's financial institution (hereafter, "bank") banks, a clearing and settlement institution, and an electronic financial message containing instructions for the transfer.[2] In a simple cross-border payment, a sender initiates a payment with their bank, followed by the sender's bank sending a financial message to the receiver's bank with information and instructions for the transaction. The receiving bank then verifies the legitimacy of the payment. Lastly, the payment is settled by a clearing and settlement institution (**Figure 1**). Processing a payment may involve only the sending and receiving banks or multiple banks if the two banks do not have a correspondent banking relationship (a formal agreement between two financial institutions to provide payment services for each other; such

[1] See more at https://www.iso20022.org/about-iso-20022.

[2] A clearing and settlement institution, which may also transmit financial messages, transfers funds and processes transactions between banks after details of the transaction are verified.

institutions typically hold accounts with each other).[3] The sending and receiving banks may exchange multiple financial messages before a transaction is settled.

Figure 1. Simple Cross-Border Payment Process



Source: Figure created by CRS.

Note: This is a simplified depiction of the cross-border payment process.

Most financial institutions use the Society for Worldwide Interbank Financial Telecommunication (SWIFT) network to send and receive financial messages for cross-border payments. Some national payment systems have their own financial messaging systems and do not use SWIFT messages.[4] For example, the Fedwire Funds Service, a real-time gross settlement system owned and operated by the Federal Reserve Banks, transmits financial messages and settles funds transfers between banks that hold accounts at the Federal Reserve Banks.[5] The system only processes transactions denominated in U.S. dollars and is mainly used for bulk transactions. The Fedwire Funds Service is only available to U.S. financial institutions, but a U.S. dollar cross-border fund transfer may involve a Fedwire message if the sending or receiving bank is a Fedwire participant. In this scenario, financial messages from multiple systems, such as SWIFT and Fedwire, may be used at different stages of the payment chain to complete the transaction.

Society for Worldwide Interbank Financial Telecommunication

SWIFT is a cooperative organization headquartered in Belgium that provides financial messaging services for financial institutions. While SWIFT provides a network for financial institutions to communicate with each other, it does not provide clearing and settlement services. SWIFT is widely recognized as being the dominant financial messaging service for cross-border payments. Although some countries have developed, or began developing, alternative systems to SWIFT (see "Changing Landscape for Cross-Border Financial Messages" below). Due to limited data availability from other financial messaging service providers, it is difficult to determine the global volume of financial messages and calculate SWIFT's precise market share.

Prior to SWIFT, cross-border payment messages were manually verified by banks using the Telex network, whose technology initially used telephone and telegraph networks combined with speech and teleprinter signals.[6] Telex was the dominant method of interbank communication from

[3] For more on correspondent banks, see CRS In Focus IF10873, *Overview of Correspondent Banking and "De-Risking" Issues*, by Rena S. Miller.

[4] Ruth Wandhofer and Barbara Casu, *The Future of Correspondent Banking*, SWIFT Institute, SWIFT Institute Working Paper No. 2017-001, October 10, 2018, p. 15.

[5] See https://www.frbservices.org/financial-services/wires/index.html.

[6] Susan V. Scott and Markos Zachariadis, "Origins of the Society," in *The Society for Worldwide Interbank Financial*

the late 1950s and throughout the 1960s. The slow and expensive process, combined with growing international trade, lack of messaging standards among financial institutions, and interest in developed a private communications network for multinational banks were the main factors in the creation of SWIFT. When SWIFT launched its first services, it introduced a central messaging platform, a computer system to validate and route messages, and a set of messaging standards.[7]

SWIFT was formed in 1973 by 239 banks in 15 countries, and is now owned by at least 2,400 financial institutions, ranging from banks, eligible securities broker-dealers, and regulated investment management institutions.[8] Its founding members provided start-up equity funding and loans when the cooperative organization was first formed.[9] SWIFT's operations have generated steady positive earnings, which covers its costs and allows the organization to return its surplus to its members through discounts and rebates to its members. Presently, SWIFT's shareholding structure is reallocated every three years and the amount of control over the organization a shareholder has is proportional to its usage of SWIFT's basic services. The shareholders elect a board, composed of 25 independent directors, that governs SWIFT and oversees its management. The National Bank of Belgium leads oversight activities with the Group of Ten (G-10) central banks to ensure its role as a "critical service provider."[10] The oversight by central banks primarily focus on SWIFT's systemic risk confidentiality, integrity, and availability.[11] The Federal Reserve Bank of New York and the Federal Reserve Board of Governors represent the U.S. Federal Reserve System in the SWIFT oversight group. In 2012, the SWIFT Oversight Forum was set up to increase information sharing on oversight activities, with an additional 15 central banks.[12]

The annual volume of financial messages (for payments, securities trade, and treasury markets) sent over the SWIFT network increased at a relatively constant rate between 2009 and 2019 (**Figure 2**). In 2019, the total number of financial messages sent was 8.4 billion, compared to 3.8 billion in 2009. The daily average number of messages was 33.5 million in 2019, compared to 14.9 million in 2009. Almost half of the messages were for payments (4.1 million). U.S. dollars had the highest share, by value, in payment messages (40.1%), followed by the European Union's Euro (34.7%). In terms of geographic regions, SWIFT processes the most payments within Europe, the Middle East, and Africa, although the payments in the Americas are also significant.

Telecommunication (SWIFT): Cooperative Governance for Network Innovation, Standards, and Community (Routledge, 2014).

[7] SWIFT, "SWIFT History," at https://www.swift.com/about-us/history, Accessed June 14, 2021.

[8] National Bank of Belgium, "SWIFT," *Financial Market Infrastructures and Payment Services Report 2019*, June 14, 2019; SWIFT, "SWIFT User Categories," at https://www.swift.com/about-us/legal/corporate-matters/swift-user-categories.

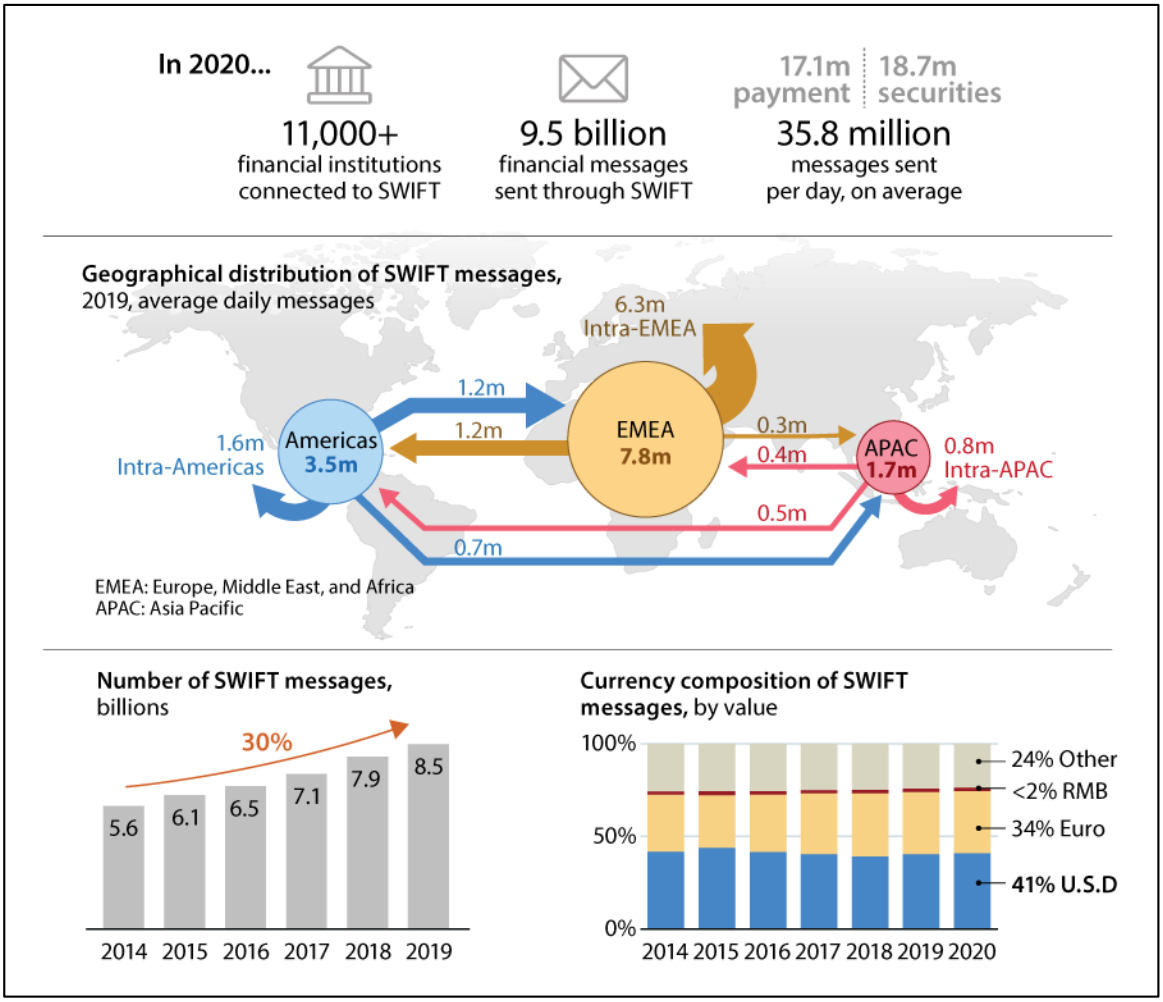
[9] Scott and Zachariadis, "How SWIFT Works," pp.29-30.

[10] G-10 central banks include Bank of Canada, Deutsche Bundesbank, European Central Bank, Banque de France, Banca d'Italia, Bank of Japan, De Nederlandsche Bank, Sveriges Riksbank (central bank of Sweden), Swiss National Bank, Bank of England, and the Federal Reserve System. "SWIFT Oversight," at https://www.swift.com/about-us/organisation-governance/swift-oversight.

[11] Scott and Zachariadis, "How SWIFT Works," p.43.

[12] The additional 15 central banks include the Central Bank of the Argentine Republic, Reserve Bank of Australia, Banco Central do Brazil, People's Bank of China, Hong Kong Monetary Authority, Reserve Bank of India, Bank of Indonesia, Bank of Korea, Bank of Mexico, Central Bank of Russia, Saudi Arabian Monetary Agency, Monetary Authority of Singapore, South African Reserve Bank, Banco de Espana, and Central Bank of the Republic of Turkey.

Figure 2. SWIFT at a Glance



Source: CRS analysis of SWIFT Annual Reviews and RMB Tracker publications, various years, available at https://www.swift.com/news-events/publications.

Notes: EMEA = Europe, Middle East, and Africa; APAC = Asia-Pacific.

SWIFT's status as the primary financial messaging service for cross-border payments is driven by the large number of banks using its network. As of December 2020, SWIFT reported that over 11,500 institutions across 200 countries and territories are connected to its network.[13] SWIFT standards are widely used among financial institutions, making it easy for users to verify each payment's information. For example, ISO has designated SWIFT with the registration authority to issue business identifier codes (BIC) to financial and nonfinancial institutions, which can be used to identify the business party, country, and branch or department of the organization. Not all financial institutions with BICs are connected to the SWIFT network, but the identifiers are used for reference purposes.[14] The large volume of financial messages that SWIFT transmits each day generates substantial amounts of financial data, which the U.S. Department of the Treasury states

[13] SWIFT, *SWIFT in Figures: December 2020 YTD*, February 2, 2021, p. 2, at https://www.swift.com/about-us/swift-fin-traffic-figures/swift-fin-traffic-document-centre.

[14] SWIFT, "What is a BIC Code?," at https://www.swift.com/standards/data-standards/bic-business-identifier-code.

is helpful in tracing financial flows and combating illicit finance.[15] SWIFT cooperates with relevant authorities, including central banks, treasury departments, law enforcement agencies, and international organizations, under specific conditions outlined in its Data Retrieval Policy, to combat illegal financial activities.[16]

Concerns and Issues Regarding SWIFT

SWIFT introduced a central platform and messaging standards for cross-border payments that previously did not exist and, as a result, increased the speed and efficiency and lowered the cost compared to the old Telex system. However, stakeholders have raised concerns and issues regarding SWIFT, including the cost and speed of cross-border payments, which are lagging behind domestic payments, as well as cybersecurity.

Cost and Speed

Cross-border payments relying on financial messages using SWIFT have been criticized as expensive, slow, and not transparent. Currently, cross-border payments largely depend on correspondent banking relationships. When the sending and receiving institutions do not have a direct relationship with each other, the payment passes through multiple banks before it reaches the intended recipient. In this scenario, SWIFT messages are sent and verified along the network of correspondent banks before the payment is processed.[17] This process results in a lack of transparency because users have been unable to follow the movement of the messages and money along the chain. In addition, fees may be incurred from each bank the payment passes through, increasing both the cumulative cost of transfer and the time it takes for the funds transfer to be completed. Each financial institution in the chain has to verify the transaction (e.g., the identity of the sender and recipient, and compliance with local financial regulations), with some users citing one to five days after initiating the transfer for the funds to be settled and available to the recipient.[18]

SWIFT has addressed concerns regarding cost, speed, and transparency in recent years. In 2017, the organization launched a new cloud-based service called the SWIFT global payments innovation (SWIFT gpi) to address transparency and costs issues. SWIFT gpi, an add-on service, offers end-to-end tracking of the movement of funds, which introduces fee transparency, and in 2019, around 50% of payments sent through gpi were reportedly available in under 30 minutes.[19] Latest information available from SWIFT states that over 1,085 banks use the service and over 75% of payment messages are sent on SWIFT via gpi.[20]

---

[15] U.S. Department of the Treasury, "Appendix D-Fundamentals of the Funds Transfer Process," *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act*, October 2006, p. 42.

[16] SWIFT, "Compliance," at https://www.swift.com/about-us/legal/compliance-0/fighting-illegal-financial-activities, Accessed June 14, 2021.

[17] U.S. Department of the Treasury, "Appendix D-Fundamentals of the Funds Transfer Process," *Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act*, October 2006.

[18] Transferwise, "How Long Does an International Wire Transfer Take?," May 2018, at https://transferwise.com/us/blog/international-wire-transfer-time.

[19] SWIFT, "SWIFT GPI Traffic Soars to $77 Trillion in 2019," March 2, 2020.

[20] SWIFT, "The Digital Transformation of Cross-Border Payments," at https://www.swift.com/our-solutions/swift-gpi/about-swift-gpi/join-payment-innovation-leaders, Accessed June 14, 2021.

Cybersecurity

The security of SWIFT's network has also been a concern in recent years after several financial institutions were the target of cyberattacks attributable to SWIFT vulnerabilities that resulted in fraudulent and unrecovered transfers, valued at millions of U.S. dollars. One particularly notable and high-profile cyberattack occurred in February 2016 when suspected North Korean hackers used SWIFT credentials of Bangladesh central bank employees to send dozens of financial messages to the Federal Reserve Bank of New York. These messages initiated transfer requests of almost $1 billion from the Bangladesh central bank's account held there.[21] About $81 million was sent to four accounts at Philippines-based Rizal Commercial Banking Corporation and $20 million to the account of a nongovernmental organization (NGO) at Sri Lanka-based Pan Asia Banking. A clerk from the Sri Lankan bank found the $20 million transfer unusual for a small NGO and contacted Deutsche Bank, which was part of the payment chain as the correspondent bank connecting Pan Asia Banking and the Bangladesh central bank, for confirmation.[22] The Bangladesh central bank sent a stop payment order after being contacted by Deutsche Bank. The Bangladesh central bank managed to stop $850 million of the initially requested $1 billion from transferring. As of 2018, about one-fifth of the $81 million sent to the Rizal Commercial Banking Corporation has been recovered. Bangladeshi officials suggested that SWIFT's integration with the central bank's real-time gross settlement system three months prior to the hack introduced security vulnerabilities.[23] SWIFT rejected the allegations, stating that the central bank is responsible for its own security.[24] In 2019, SWIFT announced it would help the Bangladesh Central Bank in rebuilding SWIFT-related infrastructure.[25]

In May 2016, Vietnam-based Tien Phong Bank announced it had prevented a similar incident during the last quarter of 2015, involving fraudulent SWIFT messages requesting transfers of over $1 million.[26] Although the SWIFT network was not directly hacked, the incidents raised concerns about hackers gaining access to valid SWIFT credentials and potentially using the system to initiate money transfers to undermine international sanctions.[27]

The Carnegie Endowment for International Peace, a foreign policy think tank based in Washington, DC, has compiled around 200 reported cyber incidents dating back to 2007 that targeted financial institutions, including payment infrastructures like national payment systems and SWIFT.[28] Between 2015 and 2020, there were nine reported incidents where hackers gained access to SWIFT's global messaging network through terminals at financial institutions (see textbox below). While none of the incidents directly compromised SWIFT's central network, the series of fraudulent transactions underscored security problems for SWIFT. While SWIFT is not responsible for the security of its users, it created a framework under its Customer Security

[21] Kim Zetter, "That Insane, $81M Bangladesh Bank Heist? Here's What We Know," *Wired*, May 17, 2016.

[22] Joshua Hammer, "The Billion-Dollar Bank Job," *New York Times*, May 3, 2018.

[23] Sanjeev Miglani, Serajul Quadir, and Jim Finkle, "Exclusive-Technicians from SWIFT Left Bangladesh Bank Exposed to Hackers-Police," *Reuters*, May 8, 2016.

[24] SWIFT, "SWIFT Statement," *Press Release*, May 9, 2016.

[25] Krishna N. Das, "SWIFT Says Helping Bangladesh Bank Rebuild Network after Cyber Heist," *Reuters*, February 2, 2019.

[26] My Pham, Mai Nguyen, and Jim Finkle, "Vietnam Bank Says Interrupted Cyber Heist using SWIFT Messaging," *Reuters*, May 15, 2016.

[27] Zetter, "That Insane, $81M Bangladesh Bank Heist? Here's What We Know."

[28] Carnegie Endowment for International Peace, *Timeline of Cyber Incidents Involving Financial Institutions*, Accessed April 12, 2021, at https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

Programme to ensure financial institutions' security measures are up to date and effective. SWIFT users are required certify that they are in compliance with SWIFT's security control framework.[29]

Reported SWIFT-related Cyberattacks

January 2015: Hackers transferred $12 million from Ecuadorian bank Banco del Austro to multiple companies registered in Hong Kong. The bank reportedly managed to recover $2.8 million. This incident is considered to be one of the first in a series of fraudulent transactions using the SWIFT network.

May 2015: Vietnam-based Tien Phong Bank announced hackers initiated SWIFT transfers valued over $1 million, but the transfer was blocked.

February 2016: Hackers, suspected to be affiliated with North Korea, initiated multiple fraudulent transfers from the Bangladesh central bank using SWIFT credentials after introducing malware to the bank's system. The requests totaled almost $1 billion and most of the transactions were blocked. However, $81 million transferred successfully to accounts in the Philippines.

July 2016: Hackers initiated transactions of $100 million from a Nigerian bank to bank accounts in Asia using methods similar to the Bangladesh hack. The money was recovered.

July 2016: Multiple fraudulent SWIFT transactions (totaling $170 million) were initiated from the Union Bank of India, but the money was recovered within three days after the incident. The methods used were similar to the Bangladesh hack earlier in the year.

October 2017: Hackers planted malware in the Far Eastern International Bank based in Taiwan to gain access to the bank's SWIFT terminal and initiated transfers of $14 million, most of it later recovered.

January 2018: Mexican state-owned bank, Bancomext, recovered $110 million in fraudulent SWIFT transactions.

February 2018: Almost $2 million worth of transactions were initiated from India's City Union Bank to accounts of correspondent banks in China, Dubai, and Turkey using the SWIFT network, but the transfers were stopped by City Union Bank and the receiving bank.

March 2018: Attackers attempted to use fraudulent SWIFT transactions to steal $390 million from the Malaysian Central Bank. Authorities stated no funds were stolen.

Source: Carnegie Endowment for International Peace, *Timeline of Cyber Incidents Involving Financial Institutions*, Accessed April 12, 2021, at https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline.

Many policy analysts warn that cyberattacks threaten the integrity of the global financial system.[30] Incidents are becoming more frequent, sophisticated, and disruptive. Cyberattacks may compromise the integrity of financial data in financial messages, causing delays in transactions. Although multiple stakeholders have started initiatives to make the global financial sector more resilient to cyberattacks, there is little international coordination among stakeholders.

Changing Landscape for Cross-Border Financial Messages

Although SWIFT has functioned as the dominant financial messaging system provider for decades, the landscape of cross-border payments infrastructure has evolved in recent years. The private sector has been developing new payments systems, primarily by using blockchain technology to create more efficient and faster payments, and that bypass the SWIFT system entirely.[31] Many central banks are exploring launching their own digital currencies, which may

[29] For more information, see https://www.swift.com/myswift/customer-security-programme-csp.

[30] Tim Maurer and Arthuer Nelson, *International Strategy to Better Protect the Financial System Against Cyber Threats*, Carnegie Endowment for International Peace, November 18, 2020.

[31] For more information on blockchain and international trade, see CRS In Focus IF10810, *Blockchain and International Trade*, by Rachel F. Fefer.

reduce or eliminate the need for financial messages. Additionally, several governments have developed, or plan to develop, their own financial messaging systems to support cross-border payments denominated in their national currencies.

In 2020, the Group of Twenty (G-20), which includes major advanced and emerging-market economies, under the Saudi Arabia presidency identified enhancing cross-border payment services a priority to support economic growth, international trade, and financial inclusion.[32]

Blockchain and Digital Currencies

A range of private-sector entities, including financial technology (fintech) startups, long-established financial institutions, and social media companies, among others, aims to decrease frictions in cross-border payments, primarily by using blockchain technology to increase security and transparency while decreasing costs and processing time of cross-border payments.

Ripple, a California-based fintech company, for example, operates a blockchain-based payments network called RippleNet. Ripple claims "hundreds of financial institutions" in over 55 countries are connected to its network and its network facilitates cross-border payments faster and cheaper than legacy systems.[33] Its network offers both financial messaging and clearing and settlement services. RippleNet's messaging system uses a decentralized network so that all users are on one platform allowing for "bidirectional messaging" and higher transparency. This allows end-users to track payment movements while decreasing costs and time for settlement. Ripple's market share in the cross-border payments market is unclear, but it has stated that its network processed almost three million transactions in 2020, nearly five times the amount in 2019.[34]

Another new payment network that uses blockchain technology is J.P. Morgan's Liink. In 2017, J.P. Morgan launched the Interbank Information Network (IIN), rebranded as Liink in October 2020,[35] as a real-time information sharing system supported by blockchain technology. J.P. Morgan claims the network has more than 400 financial institutions.[36] Cross-border payments facilitated through networks like RippleNet and Liink serve as an alternative to SWIFT.

Wide-scale adoption of digital currencies could also diminish the need for financial messaging systems. Over the past decade, the private sector has developed thousands of cryptocurrencies. A cryptocurrency is a digital representation of value generally administered using distributed ledger

[32] Bank for International Settlements, *Enhancing Cross-border Payments: Building Blocks of a Global Roadmap*, Committee on Payments and Market Infrastructures, July 2020.

[33] Ripple does not provide detailed user statistics. See more at Ripple, https://ripple.com/ripplenet.

[34] On December 22, 2020, the Securities and Exchange Commission (SEC) filed an action against Ripple for selling unregistered securities in the form of its digital asset XRP, which may impact the payment network because XRP can be used to settle cross-border transactions in lieu of fiat currency. In response to SEC's complaint, Ripple has stated that XRP has previously been classified as a digital currency by the Department of Justice and FinCEN and has been regulated as such. Ripple, "SEC Update—Preliminary Ripple Response," press release, January 29, 2021, at https://ripple.com/insights/sec-update-preliminary-ripple-response/. Securities and Exchange Commission, "SEC Charges Ripple and Two Executives with Conducting $1.3 Billion Unregistered Securities Offering," press release, December 22, 2020, at https://www.sec.gov/news/press-release/2020-338. Brad Garlinghouse, "Ripple 2020 Momentum," *Ripple*, January 25, 2021, at https://ripple.com/insights/ripple-2020-momentum/.

[35] "J.P. Morgan Adds New features to Newly Branded Liink," *Businesswire*, October 28, 2020, at https://www.businesswire.com/news/home/20201027006268/en/J.P.-Morgan-Adds-New-Features-to-Newly-Branded-Liink%E2%84%A0.

[36] J.P. Morgan, "Largest Number of Banks to Join live Application of Blockchain Technology," at https://www.jpmorgan.com/global/treasury-services/IIN.

technology and has no status of legal tender.[37] Cryptocurrencies do not rely on financial messaging services to transmit money, and they remain a small, volatile, and niche market. Some large multinational corporations are working to create more stable digital currencies for use on a larger scale, which could have a more significant impact on reducing the need for financial messaging services. For example, J.P. Morgan issued a digital coin (JPMCoin) in 2019 to be used for internal payments among institutional clients, and a consortium of companies led by Facebook is seeking to create a new global digital currency, the libra, rebranded as "diem" in December 2020, after facing scrutiny from regulators worldwide. The JPM Coin is tied to the U.S. dollar; libra/diem would be tied to a basket of currencies, including the dollar.

Many central banks are also exploring ways to create their own digital currencies, which unlike privately-issued digital currencies, would serve as legal tender and would not necessarily rely on blockchain technology.[38] According to a 2021 Bank for International Settlement (BIS) survey, 86% of the world's central banks are working on digital currencies.[39] Depending on the design features of such digital currencies, financial messenger providers like SWIFT may not be needed to complete transactions involving the central bank digital currency.

China's Cross-Border Interbank Payment Systems

The Cross-Border Interbank Payment Systems (CIPS) is a Chinese-government payment system specializing in facilitating cross-border payments denominated in China's national currency, the renminbi (RMB).[40] It was launched on October 8, 2015, to support cross-border trade, financing, and investment as part of the Chinese government's effort to internationalize the RMB.[41] Some policy analysts have stated that the slow internationalization of the RMB is partly due to the lack of the currency's full convertibility (how easy one currency can be converted into another), but CIPS and a prospective Chinese digital currency might further the use of the RMB.[42]

The China International Payment Service Corporation (CIPS Corp.), is controlled and run by China's central bank, People's Bank of China (PBOC). Financial institutions using CIPS are categorized as direct or indirect participants: direct participants hold an account with CIPS and can send or receive messages directly in the system, while indirect participants gain access to CIPS through direct participants.[43] When the system was first launched in October 2015, it had 19 direct participants and 176 indirect participants.[44] As of May 2021, CIPS has a total of 1,189

[37] For more information, see CRS Report R45427, *Cryptocurrency: The Economics of Money and Selected Policy Issues*, by David W. Perkins; CRS Report R45440, *International Approaches to Digital Currencies*, by Rebecca M. Nelson.

[38] For more information on central bank digital currencies, see CRS In Focus IF11471, *Financial Innovation: Central Bank Digital Currencies*, by Marc Labonte, Rebecca M. Nelson, and David W. Perkins.

[39] Codruta Boar and Andreas Wehrli, "Ready, Steady, Go? – Results of the Third BIS Survey on Central Bank Digital Currency," BIS Papers No. 114, January 2021.

[40] "Introduction," *CIPS*, Accessed February 10, 2021, at http://www.cips.com.cn/cipsen/7052/7057/33773/index.html.

[41] "About the System," China International Payment Service Corp., Accessed February 10, 2021, at http://www.cips.com.cn/cipsen/7052/7057/index.html.

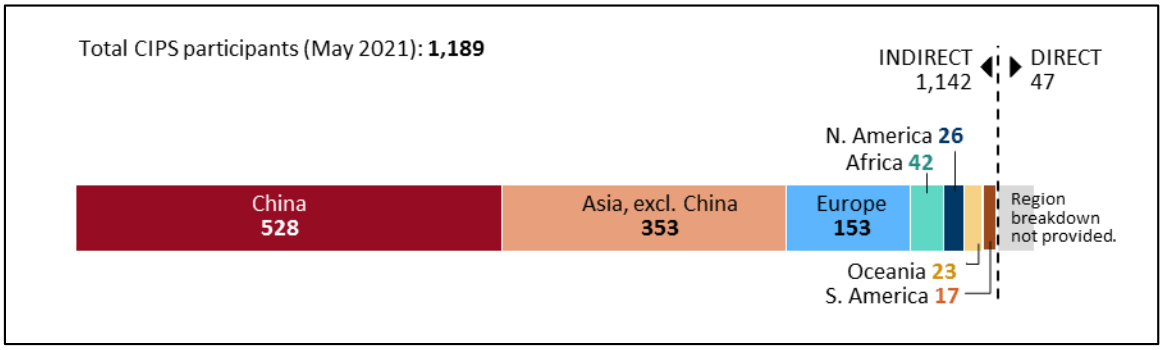
[42] "China Could Use Digital Yuan to Promote Capital Convertibility," *Bloomberg*, June 6, 2021. Rush Doshi, "China's Ten-Year Struggle Against U.S. Financial Power," *The National Bureau of Asian Research*, January 6, 2020.

[43] "Answers to Reporters' Questions about CIPS (Phase I) (October 8)," *CIPS*, December 27, 2015, at http://www.cips.com.cn/cipsen/7052/7057/33783/33822/index.html.

[44] A direct participant has a direct link to CIPS; an indirect participant does not have a direct link to CIPS but has a connection to a direct participant which exchanges with CIPS on their behalf. "Introduction," *CIPS*, Accessed February 10, 2021, at http://www.cips.com.cn/cipsen/7052/7057/33773/index.html.

participants (47 direct and 1,142 indirect).[45] Direct participants are financial institutions that must be legally incorporated in China.[46] They have direct access to the CIPS system and act as intermediaries for indirect participants for sending payment orders across the system. CIPS operates in more than 100 jurisdictions around the world, with about half of the participants located in China (**Figure 3**).

Figure 3. Cross-border Interbank Payment Systems Participants



Source: CIPS Notices and Announcements, at https://www.cips.com.cn/cipsen/7068/7047/index.html.

CIPS collaborates closely with SWIFT. CIPS relies on SWIFT's messaging services to access SWIFT's large network, although CIPS is reportedly developing the means to eventually operate independently from SWIFT.[47] In 2019, SWIFT established a wholly foreign-owned unit in Beijing in 2019 to provide localized services to Chinese users, such as services provided in local languages and customized to meet local regulatory requirements.[48] Additionally, SWIFT and CIPS established a joint venture with PBOC's digital currency research institute and clearing center in January 2021.[49] In March 2021, PBOC announced that the joint venture will set up a localized data warehouse to monitor and analyze cross-border payment messaging.[50] There is speculation about the extent to which CIPS, in the longer-term, will operate as an alternative to SWIFT.[51]

Russia's System for Transfer of Financial Messages

Russia's System for Transfer of Financial Messages (SPFS), launched in 2014 in response to U.S. and EU sanctions imposed on some trade with and investment in Russia because of its invasion of neighboring Ukraine, has been marketed as a direct alternative to SWIFT for financial messaging.

[45] "CIPS Participants Announcement No. 62," February 26, 2021, at http://www.cips.com.cn/cipsen/7068/7047/48084/index.html.

[46] See https://www.cips.com.cn/cipsen/7052/7057/33783/33822/index.html.

[47] Gabriel Wildau, "China Launch of Reminbi Payments System Reflects Swift Spying Concerns," *Financial Times*, October 8, 2015, at https://www.ft.com/content/84241292-66a1-11e5-a155-02b6f8af6a62.

[48] A wholly foreign-owned enterprise is an investment vehicle wherein non-Chinese parties (individuals or corporations) can incorporate a foreign-owned limited liability company to operate in China. A wholly foreign-owned enterprise does not require the involvement of Chinese investors, as is the case in many other investment vehicles for non-Chinese investors in China. Chen Jia, "SWIFT Opens Wholly Owned Subsidiary in China," *China Daily*, August 9, 2019.

[49] "Update 1-SWIFT Sets Up JV with China's Central Bank," *Reuters*, February 4, 2021.

[50] "China Central Bank Says New SWIFT JV Will Set Up Localized Data Warehouse," *Reuters*, March 20, 2021.

[51] Canadian Security Intelligence Service, "Beijing Creates Its Own Financial Architecture as a Tool for Strategic Rivalry," *China and the Age of Strategic Rivalry*, May 2018, p. 119.

Russia's central bank claims the network has about 400 companies.[52] In October 2019, Russian and Chinese news media reported Russia, China, and India plan to link their respective systems together.[53] Although India does not have its own cross-border messaging system, it has been reported that one is being developed.[54] Connecting their systems, the articles say, would provide users an alternative to SWIFT.

Instrument In Support of Trade Exchange

France, Germany, and the United Kingdom (E3), in 2019, formed the Instrument In Support Of Trade Exchange (INSTEX) as a special purpose vehicle to facilitate transactions with Iran.[55] INSTEX was formed after President Trump abrogated the United States' participation in the multinational nuclear agreement with Iran in 2018 and adopted a "maximum pressure" policy of sanctions on Iran. Out of concern for the United States' substantial reach and threat of secondary sanctions, SWIFT suspended some Iranian banks' access to the network, which cut off Iran from the global financial system (discussed below).[56] While INSTEX is not a financial messaging system, it provides a way for European businesses to conduct "legitimate European trade to Iran" outside of the SWIFT network.[57] The E3 created INSTEX in an effort to facilitate Europe meeting its promise under the 2015 nuclear accord to resume trade and investment transactions with Iran out of reach of U.S. sanctions. Transactions through INSTEX were initially related to the delivery of humanitarian goods, such as pharmaceuticals, medical devices, and agricultural commodities. In March 2020, INSTEX facilitated its first, and, to date, only, transaction, which exported European medical goods to help Iran combat the Coronavirus Disease 2019 (COVID-19).[58]

Cross-Border Payment Challenges and Multilateral Responses

The development of alternative financial messaging systems raises questions about how the longstanding infrastructure, including SWIFT and correspondent banking networks, will evolve, if at all. While, in general, greater competition in markets can reduce prices and improve quality for consumers, more financial messaging service providers may introduce issues of interoperability with different data standards and multiple closed systems. Furthermore, uneven application of regulatory standards across multiple jurisdictions introduces added frictions along the payment chains.

A fragmented market may introduce issues with interoperability as each financial messaging system may apply different data standards and formats. The information required and presented in

[52] Bank of Russia, "The Financial Messaging System of the Bank of Russia (SPFS)," 2020, at http://www.cbr.ru/content/document/file/72210/spfs_2020_eng.pdf.

[53] "Russia, China & India to Set Up Alternative to SWIFT Payment System to Connect 3 Billion People," *RT*, October 28, 2019, at https://www.rt.com/business/472016-russia-india-china-swift/. Chu Daye, "Payments Linkage by China, Russia and India can Challenge SWIFT Hegemony," *Global Times*, October 19, 2019, at https://www.globaltimes.cn/content/1168382.shtml.

[54] India has a domestic financial messaging system, Structured Financial Messaging System, that supports the country's real-time gross settlement and national electronic funds transfer systems. See more at https://iftas.in/services/sfms/.

[55] For more information on INTEX, see CRS In Focus IF10916, *Iran: Efforts to Preserve Economic Benefits of the Nuclear Deal*, by Cathleen D. Cimino-Isaacs, Kenneth Katzman, and Derek E. Mix.

[56] Arshad Mohammed, "SWIFT Says Suspending Some Iranian Banks' Access to Messaging System," *Reuters*, November 5, 2018. John Irish and Riham Alkousaa, "Skirting U.S. Sanctions, Europeans Open New Trade Channel to Iran," *Reuters*, January 31, 2019.

[57] "Joint Statement on the Creation of INSTEX," January 31, 2019.

[58] "Europe's Trade System with Iran Finally Makes First Deal," *AP News*, March 31, 2020.

a financial message also varies across countries and messaging systems.[59] Differing data standards and other factors, such as transmitting data in only the Latin alphabet, can prevent automated checks and delay the clearing and settlement processes. There have been efforts to introduce international standards into financial messages in order to reduce friction in cross-border payments. The ISO introduced ISO 20022 in 2004 as the "agreed methodology used by the financial industry to create consistent message standards across all the business processes of the industry."[60] ISO 20022 is not a uniform standard, but is what the ISO considers a "recipe" for financial institutions and systems to follow when developing messaging standards.[61] A number of domestic and international payment systems have adopted or are in the process of adopting ISO 20022, including SWIFT, China's CIPS, and Russia's SPFS, and Ripple.

In 2020, the Financial Stability Board (FSB)—an international body that monitors and makes recommendations about the global financial system—created a task force under the direction of the Saudi Arabia G-20 presidency to assess the existing payments landscape and develop a roadmap to enhance cross-border payments services.[62] The task force published reports that identified existing areas of friction (e.g., cost, speed, and transparency) and building blocks for further private and public cooperation, as well as multilateral cooperation, to coordinate regulatory, supervisory, and oversight frameworks.[63] The FSB published a roadmap for the G-20 with flexible goals and milestones based on the identified building blocks. Some of these goals include improving existing payment infrastructures and arrangements, such as SWIFT, while examining the potential role of services built with emerging technology (e.g., fiat currency-backed digital currencies and central bank digital currencies).

Financial Messaging Systems and U.S. Sanctions

In recent years, the U.S. government has increasingly turned to economic sanctions targeting financial institutions and transactions to advance U.S. foreign policy interests and national security. The centrality of the U.S. dollar and U.S. financial institutions gives the United States economic leverage. Congress has considered restricting sanction targets' access to financial messaging systems. SWIFT is incorporated under Belgian law, and as such complies with EU sanctions regulations as confirmed by the Belgian government. U.S. sanctions do not prohibit SWIFT from processing financial messages to or from entities designated for sanctions by the U.S. government. However, Congress authorized the use of sanctions to induce international messaging systems like SWIFT to remove certain foreign banks from its system in the case of Iran. Congress also considered such policies in the case of North Korea.

As noted earlier, some countries are creating their own financial messaging systems specifically to evade U.S. sanctions and/or reduce their exposure to future U.S. sanctions. If such alternatives

[59] Financial Stability Board, *Enhancing Cross-border Payments*, Stage 1 Report to the G20, April 9, 2020, pp. 18-19.

[60] SWIFT, "What is ISO 20022?," in *ISO 20022 for Dummies, SWIFT 5th Limited Edition* (2020), pp. 10-11.

[61] International Organization for Standardization, *Introduction to ISO 20022—Universal Financial Industry Scheme*, November 2020, pp. 4-5, at https://www.iso20022.org/sites/default/files/2020-11/Scripted_ISO_20022_ppt_long_version_v187_0.ppt.

[62] The task force—the Cross-border Payments Coordination Group (CPC)—includes the FSB, the Committee on Payments and Market Infrastructures (CPMI) from BIS, IMF, World Bank, chairs of relevant FSB groups, and the G-20 Saudi Arabia Presidency, among others.

[63] Financial Stability Board, *Enhancing Cross-border Payments*, Stage 1 Report to the G-20, April 9, 2020. Bank for International Settlements, *Enhancing Cross-border Payments: Building Blocks of a Global Roadmap*, Stage 2 Report to the G20, July 2020. Financial Stability Board, *Enhancing Cross-border Payments*, Stage 3 Roadmap, October 13, 2020.

are successful and widely adopted, the United States may not be able to leverage access to financial messaging or cross-payments infrastructure more broadly to advance its national security and foreign policy goals. During the Obama Administration, and reportedly during the Trump Administration, Treasury officials cautioned that extensive use of financial sanctions could threaten the central role of the dollar and U.S. financial system.[64]

Financial Messages and U.S. Sanctions on Iran[65]

In 2012, Congress used the threat of sanctions against SWIFT to incentivize it to disconnect the Iranian central bank and U.S.-sanctioned Iranian financial institutions. The proposed Iran Sanctions, Accountability, and Human Rights Act of 2012 (S. 2101) would have authorized such sanctions. On February 17, 2012, SWIFT announced it was ready to discontinue its services to designated Iranian financial institutions as soon as it had clarity from the EU (**Figure 4**).[66] On March 15, 2012, the EU adopted new restrictive measures on Iran and SWIFT removed the EU-sanctioned Iranian financial institutions from its system.[67] In August 2012, Congress authorized the President to impose sanctions on any specialized financial messaging systems that provided services to the Iranian central bank or specific sanctioned Iranian financial institutions (Iran Threat Reduction and Syria Human Rights Act of 2012; P.L. 112-158).

In February 2016, Iranian banks were reconnected to SWIFT following multinational sanctions relief for Iran under the 2015 Joint Comprehensive Plan of Action (JCPOA). In May 2018, President Trump announced U.S. withdrawal from the JCPOA, even as European countries continued to support it. The Administration gave a six-month wind-down period for SWIFT to remove the re-sanctioned Iranian financial institutions. If SWIFT did not remove them, SWIFT itself could have faced U.S. sanctions. In November 2018, when the wind-down ended, SWIFT announced it would disconnect the Iranian banks from its system. In its decision, SWIFT did not refer to the U.S. position but called the decision "regrettable" and "taken in the interest of the stability and integrity of the wider global financial system."[68] Given the centrality of SWIFT to the global payments system, U.S. sanctions on SWIFT would have likely created significant disturbances in the global economy. Following Iran's loss of access to SWIFT, France, Germany, and the United Kingdom developed INSTEX to facilitate economic transactions, as noted above.

[64] U.S. Treasury Secretary Jacob J. Lew on the Evolution of Sanctions and Lessons for the Future, Speech at Carnegie Endowment for International Peace, March 30, 2016; Saleha Mohsin, Nick Wadhams, and Jennifer Jacobs, "Mnuchin Feared Sanctions Would Undercut U.S. Dollar U.S. Dollar, Bolton Says," *Bloomberg*, June 18, 2020.

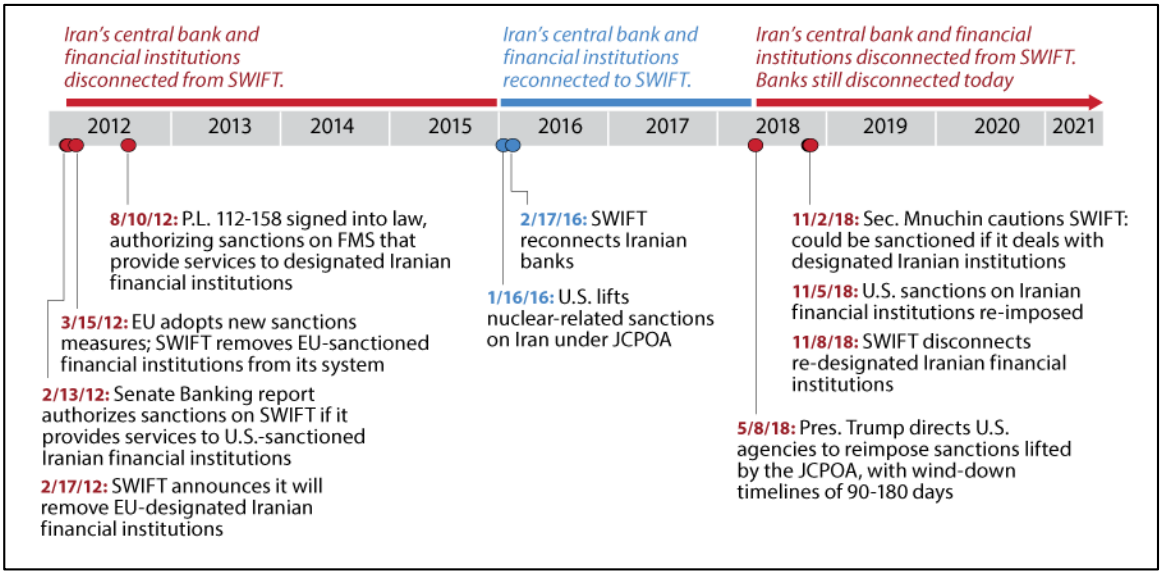
[65] For more about U.S. sanctions on Iran, see CRS Report RS20871, *Iran Sanctions*, by Kenneth Katzman.

[66] Philip Blenkinsop and Rachelle Younglai, "Banking's SWIFT Says Ready to Block Iran Transactions," *Reuters*, February 17, 2012, at https://www.swift.com/insights/press-releases/swift-instructed-to-disconnect-sanctioned-iranian-banks-following-eu-council-decision.

[67] "SWIFT Instructed to Disconnect Sanctioned Iranian Banks Following EU Council Decision," SWIFT, March 15, 2012.

[68] SWIFT and Sanctions website, at https://www.swift.com/about-us/legal/compliance-0/swift-and-sanctions.

Figure 4. U.S. Sanctions on Iran and Financial Messages: Timeline



Source: Figure created by CRS.

Financial Messages and U.S. Sanctions on North Korea[69]

In early 2017, SWIFT faced political pressures relating to North Korea, when a United Nations (U.N.) Panel of Experts report found that North Korea was relying on various companies and organizations in the international banking system, including SWIFT, to flout sanctions imposed in relation to its nuclear program.[70] Seven North Korean banks were still connected to SWIFT in early 2017, including three designated for multilateral sanctions by the U.N. Sanctions Committee overseeing North Korea-related Security Council resolutions. In early March 2017, Belgian authorities determined they would no longer allow SWIFT to provide services to North Korean banks designated under U.N. sanctions. SWIFT removed the three affected North Korean banks. The following week, SWIFT removed the remaining four North Korean banks from its system. SWIFT officially explained that the banks failed to meet its operating criteria, but did not specify what the banks' shortcomings were.[71] Experts argued that SWIFT's decision to cut off banks that were not explicitly subject to U.N. sanctions was unusual and a possible sign of diplomatic pressure on SWIFT.[72] A former SWIFT chief executive said the only previous occasion he could remember when SWIFT had cut off banks not subject to EU sanctions was when the banks had lost their banking license or a country's central bank had ceased functioning, describing it as a "very, very serious action."[73]

In July 2017, Congress passed legislation to require the President to brief congressional committees every six months on North Korea's participation in any financial messaging services

[69] For more on U.S. sanctions on North Korea, see CRS Report R41438, *North Korea: Legislative Basis for U.S. Economic Sanctions*, by Dianne E. Rennack.

[70] Hugh Griffiths, Benoit Camguilhem, Dmitry Kiku, et al., *Report of the Panel of Experts Established Pursuant to Resolution 1874 (2009)*, United Nations Security Council, February 27, 2017.

[71] "SWIFT Severs Remaining North Korean Links to Global Banking," *Financial Times*, March 17, 2017.

[72] Tom Bergin, "SWIFT Messaging System Cuts Off Remaining North Korean Banks," *Reuters*, March 16, 2017.

[73] Ibid.

(Korea Interdiction and Modernization of Sanctions Act, at Section 318; P.L. 115-44, August 2, 2017).

Other Political Pressures on Financial Messaging Providers

SWIFT has faced and resisted other calls from policymakers and government officials and interest groups to disconnect certain institutions and entire countries from its system. For example, beginning in 2004, human rights groups called on SWIFT to remove Burmese banks owned by the ruling Burmese military (Burma was ruled by a military junta that, among other actions, had rejected and annulled the results of the 1990 elections that were won by a civilian opposition party).[74] SWIFT did not disconnect the banks, maintaining its political neutrality and adherence to EU laws.[75]

In 2014, following Russia's illegal annexation of the Crimean region of Ukraine, the European Parliament passed a nonbinding resolution calling for EU members to consider excluding Russia from the SWIFT system.[76] SWIFT objected to being singled out in a European Parliament resolution, reiterated its commitment to functioning as a global and neutral provider of financial messaging systems, highlighted systems in place to facilitate its customers' compliance with sanctions and other regulations, and stated that it would not make unilateral decisions to disconnect institutions from its network as a result of political pressure.[77]

Also in 2014, SWIFT resisted calls from pro-Palestinian groups to disconnect Israeli financial institutions.[78] In 2020, some policymakers and policy experts are speculating about whether the United States should or will push SWIFT to remove Hong Kong banks from its system in response to China's moves to assert more control over Hong Kong.[79] Amidst the threat of U.S. sanctions, one of China's four large state-owned banks urged a shift from SWIFT to China's own domestic financial messaging network.[80]

More recently, in May 2021, opposition leaders in Belarus have called for disconnecting Belarus from the SWIFT system, following the forced diversion of a commercial flight under false pretenses and the subsequent removal and arrest of a dissident Belarusian journalist.[81]

---

[74] "SWIFT Runs into Political Storm over Burmese Connections," *Finextra*, June 29, 2004; Grant Peck, "Burma's SWIFT Sidestepping of Sanctions," Irrawaddy, June 29, 2004; "Crackdown: Repression of the 2007 Popular Protests in Burma," Human Rights Watch, December 2007.

[75] Ibid.

[76] European Parliament Resolution on the Situation in Ukraine and the State of Play of EU-Russia Relations (2014/2841(RSP)), September 17, 2014, at https://www.europarl.europa.eu/doceo/document/RC-8-2014-0118_EN.html?redirect.

[77] "SWIFT Statement: European Parliament Resolution," SWIFT, September 18, 2014; "SWIFT Sanctions Statement," SWIFT, October 6, 2014.

[78] "SWIFT Statement: European Parliament Resolution," SWIFT, September 18, 2014; "Financial Sanctions: The Pros and Cons of a SWIFT Response," *Economist*, November 20, 2014.

[79] Jonathan Hackenbroich, "How the US Could Ramp up its Economic War on China," European Council on Foreign Relations, July 8, 2020; Wang Yongli, "Cutting Hong Kong Off From Global Payment Network SWIFT is Next to Impossible," *Caixin Global*. July 24, 2020.

[80] "Chinese Banks Urged to Switch Away from SWIFT as U.S. Sanctions Loom," *Reuters*, July 29, 2020.

[81] E.g., see "Opposition Politician Calls for Belarus to be Disconnected from SWIFT," *Reuters*, May 24, 2021.

Selected Policy Issues for Congress

Cross-border payments make it possible for trillions of dollars of trade and investment transactions to be completed each year. The infrastructure for cross-border payments developed decades ago—relying on financial messaging services—is changing. Technological developments are creating new cross-border payments methods that could obviate the need for financial messages altogether. Additionally, some governments are developing their own financial messaging systems. As changes to the decades-old cross-border payments loom, there are a number of issues that Congress may want to consider:

- What are the benefits and costs of U.S. reliance on a widely used financial messaging system headquartered in another country? Should the United States create its own financial messaging system and/or adopt a digital dollar that reduces the need for financial messaging services?
- To what extent do new financial messaging systems, including by the governments of Russia and China, replicate the services provided by SWIFT? How does the entry of new financial messaging providers into the market impact U.S. consumers and businesses, as well as U.S. economic and foreign policy interests? What implications does the fragmentation of the cross-border payments system have for international economic stability?
- How do new technological developments interface with legacy financial messaging systems? What are the broader implications for U.S. consumers and businesses, financial market stability, and broader U.S. interests?
- To what extent, if at all, do China's and Russia's new financial messaging systems address money laundering and terrorism financing concerns?
- Is the United States able to assess the cybersecurity of financial messaging service providers in other jurisdictions? If so, how can the U.S. government ensure the level of cybersecurity is sufficient to protect U.S. consumers and businesses?
- Should the United States initiate increased multilateral cooperation on issues related to cross-border payments, such as promoting harmonizing financial messaging standards, increasing the efficiency of cross-border payments, or promoting resilience against cyberattacks?
- Do sanctions against financial service providers like SWIFT advance U.S. national security and foreign policy goals, and if so, under what circumstances? What are the benefits and costs? Do the new financial messaging systems undercut the effectiveness of U.S. sanctions? What is the impact on the use of the U.S. dollar in the global economy?

Author Information

Liana Wong
Analyst in International Trade and Finance

Rebecca M. Nelson
Specialist in International Trade and Finance

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.