

NO. 1047
JANUARY 2023

Financial Sanctions, SWIFT, and the Architecture of the International Payments System

Marco Cipriani | Linda S. Goldberg | Gabriele La Spada

Financial Sanctions, SWIFT, and the Architecture of the International Payments System

Marco Cipriani, Linda S. Goldberg, and Gabriele La Spada

Federal Reserve Bank of New York Staff Reports, no. 1047

January 2023

JEL classification: F3, F51, G15, G2

Abstract

Financial sanctions, alongside economic sanctions, are components of the toolkit used by governments as part of international diplomacy. The use of sanctions, especially financial, has increased over the last seventy years. Financial sanctions have been particularly important whenever the goals of the sanctioning countries were related to democracy and human rights. Financial sanctions restrict entities—countries, businesses, or even individuals—from purchasing or selling financial assets, or from accessing custodial or other financial services. They can be imposed on a sanctioned entity’s ability to access the infrastructures that are in place to execute international payments, irrespective of whether such payments underpin financial or real activity. This article explains how financial sanctions can be designed to limit access to the international payments system and, in particular, the SWIFT network, and provides some recent examples.

Key words: sanctions, financial sanctions, cross-border payments, SWIFT, Russia-Ukraine war

Cipriani: Federal Reserve Bank of New York, CEPR (email: marco.cipriani@ny.frb.org). Goldberg: Federal Reserve Bank of New York, CEPR, NBER (email: linda.goldberg@ny.frb.org). La Spada: Federal Reserve Bank of New York (email: gabriele.laspada@ny.frb.org). The authors thank Catherine Huang, Stone Kalisa, and Sergio Olivas for outstanding research assistance. They also thank Richard Charlton, Heidy Medina, Brett Phillips, and Janine Tramontana for helpful comments.

This paper presents preliminary findings and is being distributed to economists and other interested readers solely to stimulate discussion and elicit comments. The views expressed in this paper are those of the author(s) and do not necessarily reflect the position of the Federal Reserve Bank of New York or the Federal Reserve System. Any errors or omissions are the responsibility of the author(s).

To view the authors’ disclosure statements, visit
https://www.newyorkfed.org/research/staff_reports/sr1047.html.

When sanctions involve traded goods, it is relatively easy to understand how they function. Either certain goods are permitted to cross a national border, or they are not. In contrast, financial sanctions involve flows of funds, which occur through networks of banks and financial institutions. Financial sanctions typically restrict the ability of sanctioned entities—countries, businesses, or even individuals—to purchase or sell some financial assets. Sanctions can also be imposed on “custodial services,” which refers to the ability of entities to store or manage the financial assets of the sanctioned entity. Other financial services, such as giving financial guidance or wealth management, can also be included.

Financial sanctions have been widely used for decades. Figure 1 shows the number of sanctions episodes by 10-year periods, from 1950 through 2019. Counts of sanctions have increased over time, from 52 sanctions episodes in the 1950s to 257 in the 2010s. The sanction type indicates whether an episode is characterized by the imposition of only economic, only financial, or jointly economic and financial sanctions. The share of financial sanctions has increased: the proportion of sanctions episodes with both a financial and a real economy component increased from 12% in the 1950s to 42% in the 2010s; in contrast, exclusively economic sanctions decreased from 73% of the total in the 1950s to 41% in the 2010s. Exclusively financial sanctions were most prevalent in the 1980s and 1990s, reaching 32% of the total in the 1990s. Most sanctions are imposed by North American and European countries targeting Asian and African countries. Financial sanctions are more likely to be used than other sanctions when the goals are promoting democracy and human rights. On average, both financial and nonfinancial sanctions are imposed for shorter time periods now than in the past (Felbermayr et al., 2020).

In the last few decades a particular type of financial sanction has become more prominent: restricting access to the infrastructures and institutions that execute international payments. This type of financial sanction can potentially disrupt ev-

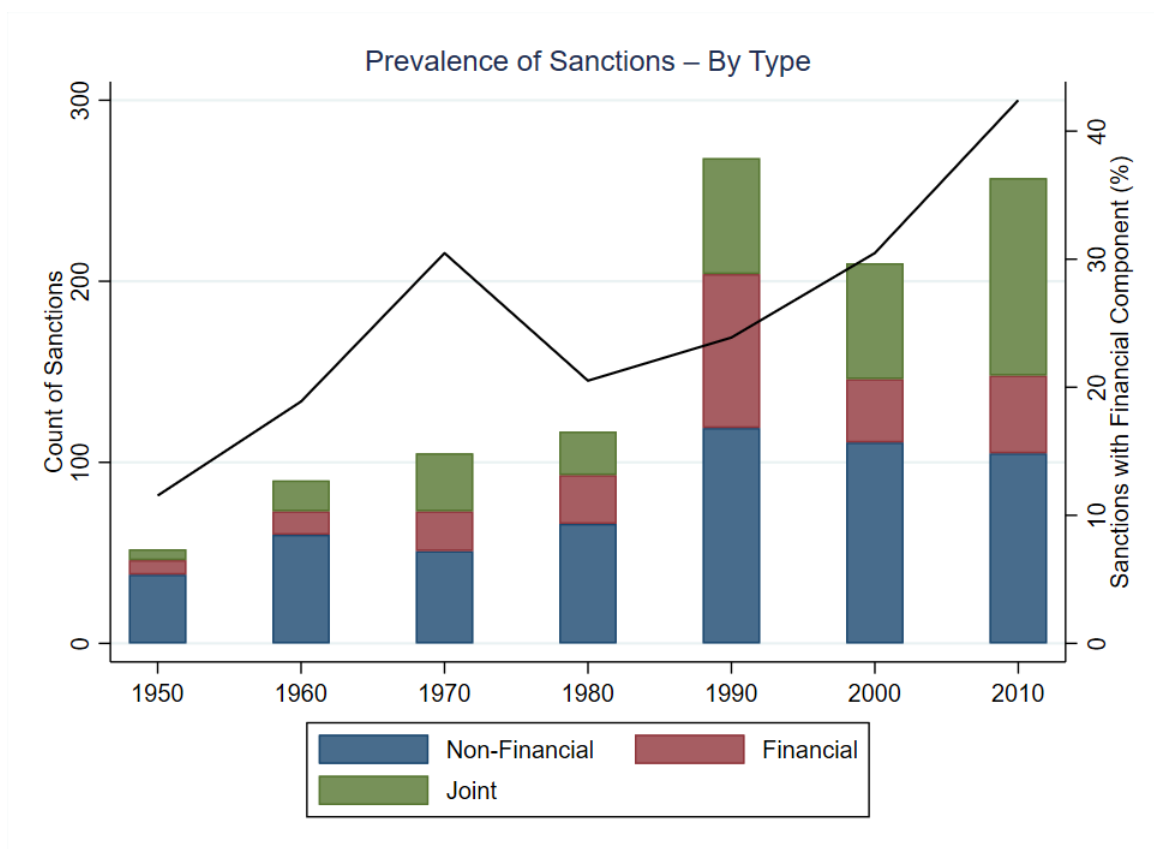


Fig. 1. Prevalence of Sanctions – By Type

Source: authors' calculations using Global Sanctions Database Felbermayr, Kirilakha, Syropoulos, Yalcin and Yotov (2020). This figure displays the number of sanctions within each decade by sanction type. Sanctions are only counted in the first decade of implementation. Joint sanctions have both economic (e.g., import restrictions) and financial (e.g., asset freezes, investment screens) elements. The black line represents the percentage of sanctions with a financial component over time (right axis).

ery kind of cross-border economic activity requiring access to the payment system, including tourism, remittances, foreign exchange trading, and international trade financing. The vast majority of communications necessary for international payments is carried over the network maintained by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), which has allowed for seamless flow of standardized information. Because there are very few alternatives to SWIFT, financial sanctions that limit access to this network have become particularly costly for sanctioned entities.

This article focuses on financial sanctions, with a particular emphasis on their relationship with the infrastructure of cross-border payments. We start with some background on financial sanctions since World War II, providing a number of specific examples of sanctions episodes along with the historical context for their imposition and the types of activities included. We then describe the infrastructure of cross-border payments, before turning to the role of SWIFT in international financial markets and the use of financial sanctions restricting access to SWIFT. We conclude by discussing some of the alternative systems some countries have created to limit the dependency on this single network. While some of these alternative systems have achieved traction within their domestic economies, they have not yet gained broad use in cross-border activity.

Examples of Financial Sanctions After World War II

Several readily accessible sources provide details on sanctioned entities – for example, governments, businesses, or individuals – and the specific activities that are forbidden, how the sanctions are implemented, and which entities are tasked with administering sanctions. Across countries, the Global Sanctions Database produced by Felbermayr, Kirilakha, Syropoulos, Yalcin and Yotov (2020) and Kirilakha, Felbermayr, Syropoulos, Yalcin and Yotov (2021) divides sanctions into economic and financial sanctions, details which countries imposed the sanctions and the sanctioned entities, categorizes the purposes of the sanctions, reports their duration, and offers an assessment of sanction effectiveness.

For the United States, the Department of the Treasury provides specifics for financial sanctions on the Office of Foreign Assets Control (OFAC) website.¹ As one example, the OFAC defines “blocking a transaction” as: “blocking a transaction in-

¹For details, see <https://home.treasury.gov/policy-issues/office-of-foreign-assets-control-sanctions-programs-and-information>.

volves accepting or segregating the funds or securities associated with the transaction and then freezing those funds, securities or accounts so that the owner is effectively denied access until appropriate action is taken by OFAC. Blocking can occur when a transaction is initiated at an institution or when funds or securities are moved through an institution during a transfer.”

The remainder of this section describes specific episodes of financial sanctions, explaining how and why sanctions were imposed, with the purpose of outlining the different forms that financial sanctions can take and how they have evolved over time.

US Sanctions against North Korea in the 1950s

In June 1950, North Korea invaded South Korea; in response to this attack, on June 25 and 27, the United Nations Security Council passed Resolutions 82 and 83, sponsored by the US, calling for North Korean authorities to withdraw, and recommending urgent military measures by UN members. The US imposed sanctions against North Korea in the 1950s, with the purpose of helping the US win the Korean War.

The US sanctions had both trade and financial components. The trade restrictions, such as a total embargo on exports to North Korea, were instituted just three days after the outbreak of the war (June 28). In addition to the embargo, the Department of the Treasury issued the Foreign Assets Control Regulations (FACR) in January 1951, forbidding any financial transactions involving North Korea and its nationals. Moreover, the Department froze North Korean assets held under US jurisdiction (see Chang 2006). China, a North Korea ally in the war, was also subject to the same sanctions.

The US did not impose restrictions on North Korean’s access to the infrastructure allowing international payments and financial transactions; rather, they made such

transactions illegal for US residents. Financial sanctions against North Korea are an example of sanctions where financial transactions and ownership of financial assets are impaired, but access of the country to the infrastructure of payment system is not affected.

US Sanctions against Chile from 1970 to 1973

In the 1960s, Chile received extensive credit from the US and from international organizations based in the US, such as the Inter American Development Bank. Indeed, in 1970, 60% of Chile's debt was owed to the US government (Helwege 1989). Moreover, in the late 1960s, private credit from the US had become increasingly important, with US commercial banks providing significant lines of credits.

In 1970, Salvador Allende won the Chilean presidential election and started pursuing domestic and international policies contrary to US interests in the region. Between 1970 and 1973, the US put in place a series of economic measures against Chile which became known as "the invisible blockade," aimed at destabilizing the country and overthrowing Allende (Petras and Morley 1975, Petras and Morley 1978, and Olson 1979).

In addition to trade restrictions, financial activity between the US and Chile decreased significantly. The US tightened official-sector credit flows towards Chile: US-AID loans were reduced from \$45 million in 1969 to \$1.5 million in 1971; Import-Export Bank credits evaporated entirely. In addition, the Inter-American Development Bank reduced the credit provided to Chile from \$46 million in 1970 to \$2 million in 1972 (Livingstone 2009).

US private financing also declined dramatically: short-term lines of credit from US private banks declined to around \$30 million, and short-term US commercial credits dropped from 78.4 percent of the total in 1970 to approximately 6.6 percent in 1972 (Petras and Morley 1975 and Petras and Morley 1978). Additionally, US suppliers

were demanding “cash in advance” for essential raw materials and parts sales to Chile, putting further pressure on Chile’s finances (Petras and Morley 1975, Olson 1979, and Livingstone 2009). The reduction in private-sector lending may have been due both to the nature of the policies put forward by the Allende government which were generally not business friendly (e.g., completing the nationalization of American copper companies in Chile that began in 1965) and to the desire of US financial institutions to be aligned with the policies of the US government (Sigmund 1974 and Petras and Morley 1978).

As in the case of the sanctions against North Korea, the US did not target the infrastructure of financial transactions. Different from the North Korean case, however, the US did not adopt explicit measures forbidding financial transactions between the US and Chile or freezing the US financial assets owned by Chilean residents. Instead, the US government relied on the economic disruption brought forward by a little-publicized reduction in both official-sector and private-sector lending to the country (Olson 1979). The US economic pressure on Chile ended after the military coup that overthrew the Allende’s government in late 1973.

European and US Sanctions against South Africa in the 1990s

Since the early 1960s, the United Nations (UN) and many countries called for and implemented economic sanctions against South Africa in order to pressure the South African government to abandon its apartheid policy of racial segregation (Crawford and Klotz 1999). In 1963, the UN Security Council adopted a voluntary arms embargo, which it made mandatory in 1977. In November 1973, the OPEC countries extended their oil embargo to South Africa.

Although some financial sanctions were put in place in the 1960s and 1970s (e.g., Japan banned direct investment in 1964 and then loans in 1975), more extensive financial sanctions were introduced during the South African debt crisis of 1984-1985,

along with a tightening of trade-based economic sanctions. In 1986, the European Community, the US, and Japan sanctioned import of gold coins (the Krugerrand) and certain steel and iron products. However, most forms of gold, which accounted for 42.6% of the value of South African merchandise exports, were not sanctioned (Crawford and Klotz 1999 and Levy 1999). Financial sanctions mainly focused on foreign direct and portfolio investments in South Africa. The European Community sanctioned new direct investments, but member states were not required to impose binding sanctions; indeed, Great Britain and Germany – the two major investors in South Africa – decided not to do so (Crawford and Klotz 1999, (Becker 1988), and Hefti and Staehelin-Witt 2011). The US sanctioned new direct investments through the Comprehensive Anti-Apartheid Act (CAAA) of 1986, along with portfolio investments and credits and loans; the CAAA also prohibited US banks from accepting deposits from South African government agencies (Becker 1988).

The South African apartheid regime ended with the general election of 1994. Similarly to the US sanctions against North Korea, the 1980s financial sanctions against South Africa did not involve the infrastructure of cross-border payments; indeed, they were more limited than sanctions on North Korea, targeting mainly foreign direct investment into South Africa. Moreover, similar to other cases described above, sanctions were accompanied by significant actions by non-government actors, such as divestment by US universities and pension funds from companies doing business in South Africa. As a result of both pressure from the anti-apartheid movement and the concerning conditions of the South African economy, several banks and multinational companies disinvested from South Africa in the 1980s. For example, in July 1985, Chase Manhattan Bank decided not to extend credit or to make new loans to South Africa; immediately after, other international banks and investors moved their funds out of the country, leading the Johannesburg Stock Exchange (JSE) to drop sharply and the rand to plummet. In 1986, in response to customer pressures,

Barclays Bank ended its loans to South Africa and withdrew from South African operations. In the same year, General Motors withdrew from South Africa, followed by many other US corporations (Crawford and Klotz 1999).

Although the sanctions' goal was ultimately achieved, the contribution of foreign economic and financial pressures to the regime downfall is still debated (Levy 1999). During the sanctions period (1986Q4 to 1991Q1), South Africa suffered an average net capital outflow of 2% of South African GNP. However, this is mostly attributed to poor economic conditions, rather than to the impact of sanctions. Indeed, although sanctions made capital scarce, the annual cost to the South African economy is estimated at less than 0.25% of South African GNP; the relatively low effectiveness is attributed to the lack of sanctions by the UK and Germany, to the fact that sanctions did not cover reinvested profits (80% of FDI into South Africa), and to the fact that only the US sanctioned portfolio investment (Hefti and Staehelin-Witt 2011).

EU and US Sanctions against Myanmar in the 1990s and 2000s

In the 1990s and 2000s, the EU and US adopted several economic sanctions against Myanmar in response to systematic violations of human rights and civil liberties by the country's ruling military junta. In 1991, the EU imposed an array of traditional economic sanctions, including an arms embargo, a suspension of bilateral aid, and a visa ban on Myanmar officials (Giumelli and Ivan 2013). In 2000, the EU strengthened the existing economic sanctions and added a financial component, freezing the funds held abroad by the persons included in the visa ban. In 2004, the EU imposed restrictions on EU investment into Myanmar, in particular into Burmese state-owned firms (European Commission 2005). Similar restrictions on investment into Myanmar were introduced by the US. Finally, Canada, the EU, and the US stopped providing preferential financing for exports to or investment in the country

(Martin 2012).

Myanmar is a significant example of international pressure to impose restrictions on the country's access to the infrastructure of the financial system. Beginning in 2004, human rights groups, such as Human Rights Watch, urged SWIFT to remove Myanmar banks owned by the ruling military junta from its network, pointing out that the military dictatorship could use the network to evade the economic and financial sanctions. In this instance, SWIFT refused to disconnect the banks, in order to maintain an apolitical posture, on the ground that no EU law restricted access to SWIFT by Myanmar (Wong and Nelson 2021).

US Sanctions against Afghanistan in the 2000s

In the late 1990s and early 2000s, several countries and international organizations imposed important economic and financial sanctions against the Taliban regime ruling Afghanistan. The goal of these sanctions was to force the Afghan government to stop sheltering and training terrorists. These sanctions were aimed at putting pressure not only on segments of the economy but also on specific individuals. An example of financial sanctions imposed against Afghanistan is US Executive Order No. 13129, issued in July 1999, banning all trade with Taliban-controlled areas, freezing Taliban assets in the US, and prohibiting financial contributions to the Taliban (Hufbauer, Schott and Oegg 2001).

Shortly afterwards, in October 1999 and December 2000, the UN Security Council adopted two rounds of sanctions against the Taliban regime (Council Resolutions 1267 and 1333; see Francioni and Lenzerini 2003 and Ghufuran 2001). The Council's actions included travel bans, an arms embargo, and a ban on exports of acetic anhydride, used to manufacture heroin (of which Afghanistan is the world's largest producer). Finally and most importantly, these sanctions froze funds and other financial assets, owned directly or indirectly, by the Taliban, Osama bin Laden, and

individuals transacting with him. One of the main goals of these sanctions was to coerce the Taliban to hand over Osama bin Laden. The effectiveness of these sanctions, however, is still debated, as the Taliban did not turn over bin Laden nor did al-Qaeda stop its terrorist activity.

Sanctions against Afghanistan intensified after the September 11, 2001 attacks. On September 23, 2001, to weaken the financial support of al-Qaeda, the US President issued an executive order expanding the list of individuals and entities subject to the asset freeze, including fundraising organizations (Hardister 2002). Reducing the financial capabilities of terrorist organizations was seen as a key component of the “war on terrorism.” Moreover, the US created the Foreign Terrorist Asset Tracking Center in the Treasury Department to coordinate the activities of the US agencies on the financial front.

Importantly, the US “war on terrorism” included a covert monitoring of global financial transactions through the SWIFT network (Connorton (2007); Koppel 2011). In October 2001, the US Treasury established a secret program later referred to as the “Terrorist Financing Tracking Program” (TFTP) but more commonly known as the “SWIFT Program” through which the Office of Foreign Assets Control (OFAC) would issue subpoenas to the SWIFT data processing center in the US. The amount and type of data accessed by US authorities is not publicly known. As SWIFT acknowledged, initially the scope of US searches covered the entire SWIFT database, with the transfer to the US Treasury of all messages within a certain time period. Subsequent subpoenas, however, were narrower and limited to specific dates and countries of origin or destination (Koppel 2011). According to US Treasury officials, in 2007-2008, US counter-terrorism analysts at the CIA (in charge of extracting individual-level information from the SWIFT messages) searched less than one percent of the subset of SWIFT messages sent to the US Treasury (Amicelle 2011).

The existence of the program became public in 2006, following a series of articles

in major US newspapers. Although the program was legal under US law, it generated controversies both in the US and EU because of its implications for privacy and civil liberties (de Goede 2012). In particular, the Treasury received details about millions of messages, including senders' and receivers' personal data. Although the data were obtained from the US-based SWIFT operating center, they contained information on non-US citizens too and European authorities expressed serious concerns regarding possible violations of European privacy law (Amicelle 2011; Koppel 2011; de Goede 2012). Negotiations between the US and EU, combined with mounting media pressure, led to an agreement on the SWIFT surveillance program between the US and the EU in June 2007, limiting the use of the data by US authorities for counterterrorism purposes, limiting the retention period for the data to 5 years, and allowing monitoring of the program by EU officials (Connorton (2007); Koppel 2011).

Moreover, EU pressures led SWIFT to improve its data protection standards and to create two message-processing zones: one in Europe (with processing centers located in the Netherlands and Switzerland) and one in North America (with processing centers located in the Netherlands and the US), thereby separating EU traffic and US traffic. Countries have the option to choose which processing zone (and therefore pair of processing centers) they want to belong to. This change means that all traffic within the European processing zone, to which most countries have opted to belong, is not accessible by US surveillance.

The Infrastructure of Cross-border Payments

Cross-border payments infrastructures are a critical component of how governments, companies, and households actually can pay for their international purchases, whether of goods, services, or financial assets. Once we understand this infrastructure, it becomes clear why restricting access to the infrastructure has been part of

several sanction packages, especially in the most recent years, including the 2022 sanctions against Russia discussed in “The Role of SWIFT in the Implementation of Financial Sanctions” section.

Payments within a single country typically settle on the books of commercial banks or of the central bank. For instance, if entity A wants to send funds to entity B, A will instruct A’s own bank, which will make a payment to B’s bank. If both A and B are customers of the same bank, the payment can be settled on the bank’s own books. If, however, A and B are customers of different banks in the same country, the settlement will typically occur on the books of the central bank. Many central banks, in fact, have set up “real-time gross settlement” (RTGS) systems that allow the settlement of payments between banks in real time, on a gross basis. In the United States, Fedwire Funds Services is a notable example. In the case of A and B just described, the payment will result in a decrease of the account balances of A’s bank with the central bank and an increase in the account balances of B’s bank.

Now consider cross-border payments, which are payments between residents located in different countries. Few central banks allow their domestic payment system to be accessed by banks that do not have a physical presence within the country and that are not subject to the country’s regulation and supervision; a notable example is the Swiss National Bank, which allows institutions without a presence in the country to access its real-time gross settlement system (Swiss Interbank Clearing). Traditionally, however, cross-border payments occur through “correspondent banking”: banks use the services of “correspondent banks” in order to execute cross-border payments (Bank for International Settlements 2016). The correspondent bank is usually either a large bank or a local branch/subsidiary of the bank initiating the payment, located in the foreign country where the payment must be sent. Banks may have more than one correspondent bank in a given country.²

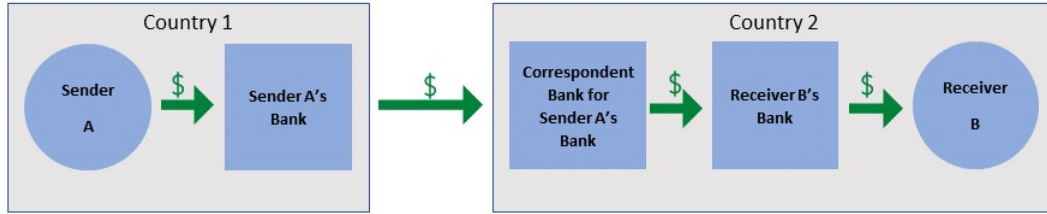
²Correspondent banking is also used for domestic payments when a bank does not have an account

A “correspondent account” is an account that a “respondent bank” has at a foreign correspondent bank, usually in the foreign bank’s currency. Both banks will keep a record of this account, and common terminology here is to refer to *Nostro* and a *Vostro* accounts, where the terms are the Italian words for “ours” and “yours.” The record kept by the respondent bank of the money that it keeps with its correspondent bank is the *Nostro* account, whereas the record kept by the correspondent bank of its respondent bank’s money is the *Vostro* account. Panel (a) of Figure (2) illustrates how a correspondent-bank relationship would allow a payment between parties A and B in different countries. In this example, if A wants to send money to B, who resides in another country, A’s bank will instruct its correspondent bank in the country where B resides to send money to B’s bank through the domestic payment system of B’s country. The *Nostro* account of A’s bank (an asset on the bank’s balance-sheet) will be debited for the amount paid; similarly, the *Vostro* account (a liability on the correspondent bank’s balance sheet) will also be debited.

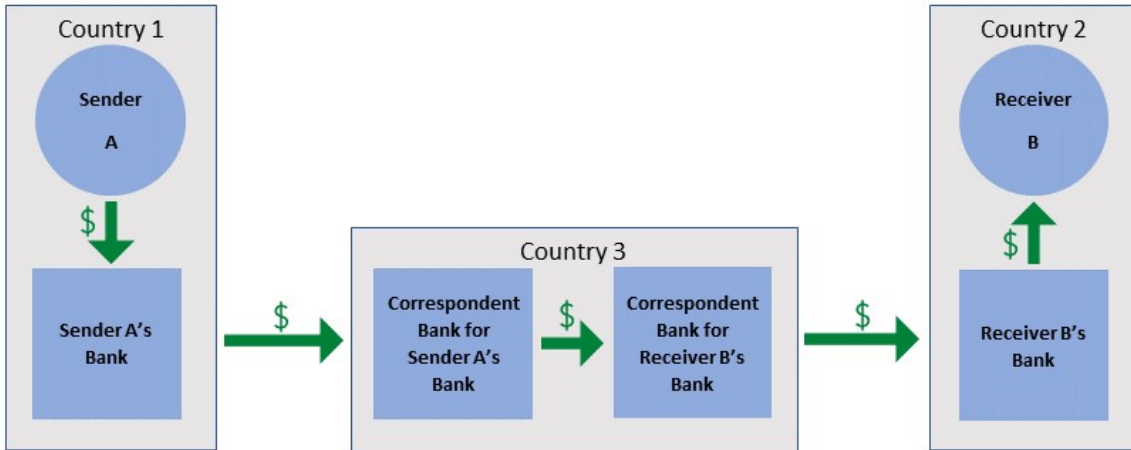
Cross-border payments through a correspondent banking relationship may be more complex than in the previous example and involve more than one intermediary. For instance, say that A and B agree that the payment should be in a third country’s currency. As shown in Panel (b) of Figure (2), A’s bank will instruct its correspondent bank in the third country to transfer funds (through the third country’s domestic payment system) to the correspondent bank of B’s bank in the third country. In some cases, many correspondent banks are involved in the settlement of a payment. As correspondent banks are compensated for their correspondent services, the higher the number of banks involved, the higher the cost of the transaction.

Correspondent banks typically perform their own diligence for anti-money laundering (AML) and countering the financing of terrorism (CFT) purposes based on

with the central bank; for instance, in the US, community banks and credit unions often do not have accounts with the Federal Reserve.



(a) Two countries



(b) Three countries

Fig. 2. Cross-border payments and correspondent banking

Source: Authors' construction. Panel A shows the flows in a cross-border payment executed through a correspondent bank. Panel B shows the flows in a cross-border payment executed through correspondent banks domiciled in a third country.

the requirements of their jurisdictions. The Financial Action Task Force (FATF), an intergovernmental organisation established in 1989 by the G-7, develops AML/CFT guidance on effective supervision and enforcement. Normally, AML/CFT policies do require institutions to conduct due diligence on their respondent banks but not on the customers of their respondent banks; nevertheless, correspondent institutions are usually required to monitor respondent banks' transactions "with a view to detecting any changes in the respondent institution's risk profile or implementation of risk mitigation measures" (FATF 2016). For instance, in the US, banks are generally required to collect information on the origin and the recipient of transactions. Sometimes, correspondent banks may be held liable by the authorities of the country where they are located for violations of AML/CFT laws or regulations by their

respondent banks.

Compliance with AML/CFT laws and regulations often makes correspondent banking relationships very costly for the correspondent bank. This is especially true if the respondent bank is located in a small country, where the volume of transactions is low, or in a country deemed at high risk for AML/CFT compliance. The high cost and low profitability have resulted in a decrease in the number of correspondent banking relationships over the last decade, a phenomenon called “de-risking” (Grolleman and Jutrsa 2017; Miller 2022). The number of active correspondent banks worldwide fell by roughly 22 percent between 2011 and 2019, with banks losing correspondents even as the value of cross-border payments continued to grow; the decline has been especially pronounced in Latin America. At the same time, the number of country-pairs linked by a correspondent relationship the so-called “corridors” has decreased by ten percent, leaving some regions, especially in Latin America, Oceania, and Africa, with very few corridors (Rice, von Peter and Boar 2020 and Bank for International Settlements 2020).

The reduction in correspondent banking relationships implies that some cross-border payment activity, especially if it involves small countries, needs to go through a longer chain of banks, potentially increasing the cost to end-user. Although comprehensive data on the cost of correspondent banking is lacking, the World Bank collects data on the cost of migrants’ remittances, with the aim of reducing it to promote financial inclusion; although the cost of remittances from G20 countries has been steadily decreasing since the 2010s, the concern is that de-risking by banks may slow down the process, or even lead to higher remittance costs in some countries (World Bank 2022).

The high cost of correspondent banking activities has also led to the development of alternative arrangements to facilitate payment activity between residents of different countries (see Bech and Hancock (2020) for a detailed analysis of these

arrangements). These arrangements may be sponsored by a single country or may be the result of multilateral agreements among a group of countries. For instance, a country may want to allow its residents to send and receive payments from a larger economy or currency area. One example is Switzerland, which established the Swiss Euro Clearing Bank (SECB) to allow its residents to send and receive euro payments from the European Union. Similarly, the Central Bank of Mexico, in a joint effort with the Federal Reserve, established “Directo a Mexico” to connect its own payment system to that of the United States.

Conversely, a country may want to set up a system to facilitate the use of its own currency by foreign residents or to facilitate regional transactions. As a prominent example, in 2015, China established the Chinese Cross-Border Interbank Payment System (CIPS) to facilitate the use of the renminbi in international transactions. As CIPS has developed a messaging system alternative to SWIFT, we will discuss it at more length in the next section, which describes the SWIFT messaging network and its origins, as well as its use in financial sanctions.

Sometimes, a group of countries, usually neighbors, may jointly develop a payment system to allow their residents to transact among themselves; for example, the Southern Africa Development Community, a group of 16 countries in southern Africa, set up its own real-time gross settlement system for transactions in South African rand. Another example is the East Africa Payment System (EAPS), which offers multi-currency payments for countries in the East Africa Community, which includes Burundi, Kenya, Rwanda, Tanzania, and Uganda.

Even if both parties to a transaction are residents of the same country, there are cases in which payment in another country’s currency may require the costly intermediation of correspondent banks. This friction has prompted some jurisdictions to set up “offshore” payment systems, processing payments in a currency different from that of the country where the payment system is based. For instance, Hong

Kong has set up parallel real-time gross settlement systems that, in addition to the Hong Kong dollar, will also settle payments in euros, US dollars, and renmimbi.

Finally, foreign-exchange transactions pose a particular type of settlement risk as they require the payment of an agreed amount in one currency against an agreed amount in another currency.³ What is called “payment vs. payment” settlement mitigates settlement risk by only allowing two legs of a foreign-exchange transaction to settle contemporaneously. The CLS Bank, based in the United States, is a specialized financial intermediary set up in 2002 to allow the settlement of foreign exchange transactions on a payment vs. payment basis; it currently allows for foreign-exchange transactions in 18 currencies (Galati, 2002).⁴ CLS has 70 members, which are major financial institutions that hold accounts with CLS, and it settles the transactions between its members on its books.

A History of SWIFT

In the middle of the twentieth century, banks had been communicating nationally and internationally through Telex. For readers who have not yet reached retirement age, the Telex is a teleprinter network that originally used existing telegraph and telephone networks and allowed speech and teleprinter signals on the same connection. Introduced in the 1930s, the Telex quickly replaced the telegram in business use and grew fast in popularity: by 1957, there were more than 30,000 users worldwide, and in the late 1970s, more than one million. However, Telex messages were costly and carried high operational risk: because Telex communication allowed to

³Settlement risk in foreign-exchange transaction is usually referred to as “Herstatt Risk:” in 1974, Herstatt Bank, a German bank active in foreign-exchange trading, was closed by German authorities after it had received payments for foreign-exchange transactions, but before it could make the outgoing payments, leading to a freeze in the foreign-exchange market.

⁴The 18 currencies are: Australian dollar, Canadian dollar, Danish krone, euro, HK dollar, Hungarian forint, Israeli shekel, Japanese yen, Mexican peso, New Zealand dollar, Norwegian krone, Singapore dollar, South African rand, South Korean won, Swedish krona, Swiss franc, Pound sterling, US dollar.

send unformatted texts with no pre-specified standard, a cross-border transaction would often require the exchange of more than ten messages and authentication procedures between banks were also labor intensive (Scott and Zachariadis, 2012).

By the early 1970s, there was a growing presence of European and US banks in overseas markets and a rise in cross-border payment activity. Banks began looking for ways around the high costs and other limitations of Telex. In one prominent example, in 1973, Citibank's information technology subsidiary (Transaction Technology Inc.) developed a proprietary messaging system called MARTI (Machine Readable Telegraphic Input). By mid-1974, this network was in place and a pilot implementation had been conducted with one of Citibank's correspondent banks, Wilmington Trust. Citibank tried to force the adoption of MARTI on other correspondent banks, both in the United States and Europe, announcing that the deadline for compliance would be March 31, 1975. Many correspondent banks, particularly in Europe, resisted the imposition of a proprietary standard from a single bank (Scott and Zachariadis, 2014). Indeed, European banks feared the establishment of a US-led monopoly for the transmission of financial information.

Thus, in 1973, 239 banks from 15 countries founded SWIFT, the Society for Worldwide Interbank Financial Telecommunication, as a non-profit financial institution. The goal was to create a data processing and messaging network that would be shared among banks worldwide, with standards collectively designed by private companies for community purposes (Scott and Zachariadis, 2014). SWIFT is headquartered in Belgium and is organized as a cooperative society owned by its members; membership was originally limited to banks but is now open to broker-dealers and investment-management institutions.⁵

Figure 3 shows the role of SWIFT in the correspondent bank transaction we

⁵For details, see the SWIFT website at <https://www.swift.com/about-us/legal/corporate-matters/swift-user-categoriesshareholding-eligibility>.

described earlier and illustrated in Figure 2. The primary role of SWIFT is as a message carrier: the SWIFT network securely transports messages containing the payment instructions between financial institutions involved in a transaction. In addition to providing the messaging network for financial transactions, SWIFT offers a secure person-to-person messaging service for the transfer of sensitive business documents, for example, contracts and invoices.

Importantly, SWIFT is not a bank and does not manage accounts or hold funds on behalf of its customers. Neither is it a clearing or settlement institution. SWIFT only provides the platform allowing the secure exchange of financial information and proprietary data across financial institutions worldwide. Namely, SWIFT provides two main services to the financial sector: (1) a secure network for transmitting messages between financial institutions and (2) the development and maintenance of a set of syntax standards for financial messages (Scott and Zachariadis, 2012). For this reason, SWIFT does not eliminate the role of correspondent banks and other institutions involved in the settlement process.

SWIFT's messaging network is run from three data centers, located in the United States, the Netherlands, and Switzerland.⁶ SWIFT uses undersea fiber-optic communications cables to transmit financial data across countries (Sechrist, 2010). The CLS Bank, which as we described earlier operates the largest multi-currency cash settlement system, conducts millions of transactions and trades worth trillions of US dollars a day on the same undersea cables. SWIFT's data centers share information in near real-time; in case of a failure in one of the data centers, the other centers are able to handle the traffic of the whole network.

The other fundamental purpose of SWIFT has been the development of a set of syntax standards that would facilitate financial transactions, overcoming the high

⁶As we mentioned above, these three centers create two separate message-processing zones in Europe and in North America.

processing costs and low reliability associated with Telex and easing information transmission. New standards are continuously developed and replace older ones. For example, ISO 9362, developed in 1994, defines a standard format for Business Identifier Codes (BIC) to uniquely identify financial and non-financial institutions worldwide; ISO 10383, developed in 2003, defines codes for exchanges and market identification; ISO 13616, developed in 2003, defines the International Bank Account Number (IBAN) to uniquely identify bank accounts worldwide; and ISO 20022, developed by updating earlier standards in 2004 and 2007, defines a universal message scheme for electronic data interchanges between financial institutions, including payments, credit and debit card transactions, and securities trading and settlement. These formats are currently the main standards used in financial transactions.

SWIFT's standardization of financial messages has become the most influential and widely-used in the financial industry. Indeed, the International Organization for Standardization (ISO) appointed SWIFT as the Registration Authority (that is, the entity responsible for defining and maintaining the rules) for several ISO standards. Currently, there are nine broad categories of SWIFT messages, ranging from funds transfers to foreign exchange transactions.⁷ Table A1 in the appendix shows a fictitious example of transaction involving one of SWIFT's most common messages, the MT103 funds transfer message.

⁷These categories are; Customer payments and cheques (MT1XX), Financial institution transfers (MT2XX), Treasury markets - Foreign exchange and derivatives (MT3XX), Collection and cash letters (MT4XX), Securities Markets (MT5XX), Treasury markets - Precious metals and syndications (MT6XX), Documentary credits and guarantees (MT7XX), Traveller's cheques (MT8XX), and Cash management and customer status (MT9XX).

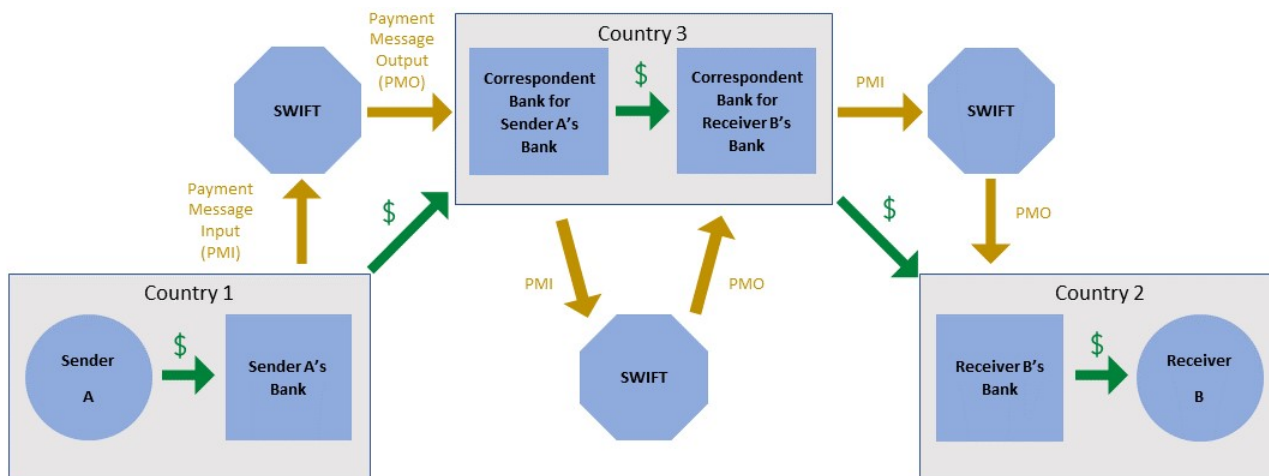


Fig. 3. The role of SWIFT in cross-border payments

Source: Authors' construction. This figure replicates Panel B of Figure 2 highlighting the role of the SWIFT network in facilitating cross-border payments.

Although SWIFT shareholders can only be banks, broker-dealers, and investment management institutions, the network can be used by a much broader set of institutions, including any supervised financial institution, international or intergovernmental bodies involved in finance and payments, non-supervised financial institutions, corporations, financial market regulators, payment systems, and security-market infrastructures.⁸

As Figure 4 shows usage of the SWIFT network has grown steadily: in 2020, more than 11,000 institutions, located in more than 200 countries, were connected to SWIFT. In 2020, more than 9.5 billion messages were sent through the network, with an average daily volume of 37.7 million messages. Roughly 49 percent of this traffic was for securities trading and 45 percent for payments. The share of messages regarding securities trading has steadily been increasing over time, going from 40 percent in 2007 to almost 50 percent in 2020. Twenty-seven percent of the traffic originated in the Americas, 59 percent in the region comprising Europe, the Middle

⁸For detailed user and shareholder eligibility criteria see: <https://www.swift.com/node/7776>. The expansion of the eligibility criteria to use SWIFT started in the late 1980s. Today shareholders represent only roughly one fourth of users.

East, and Africa, and the rest in the Asia-Pacific region (SWIFT, 2020). At the end of 2020, 39 percent of total payment value was sent in US dollars and 37 percent in euros; in terms of trade finance, the US dollar represented 86 percent of the value of SWIFT traffic, whereas the euro represented only 7 percent, with the Chinese renminbi amounting to 2 percent of the total value (SWIFT, 2021).

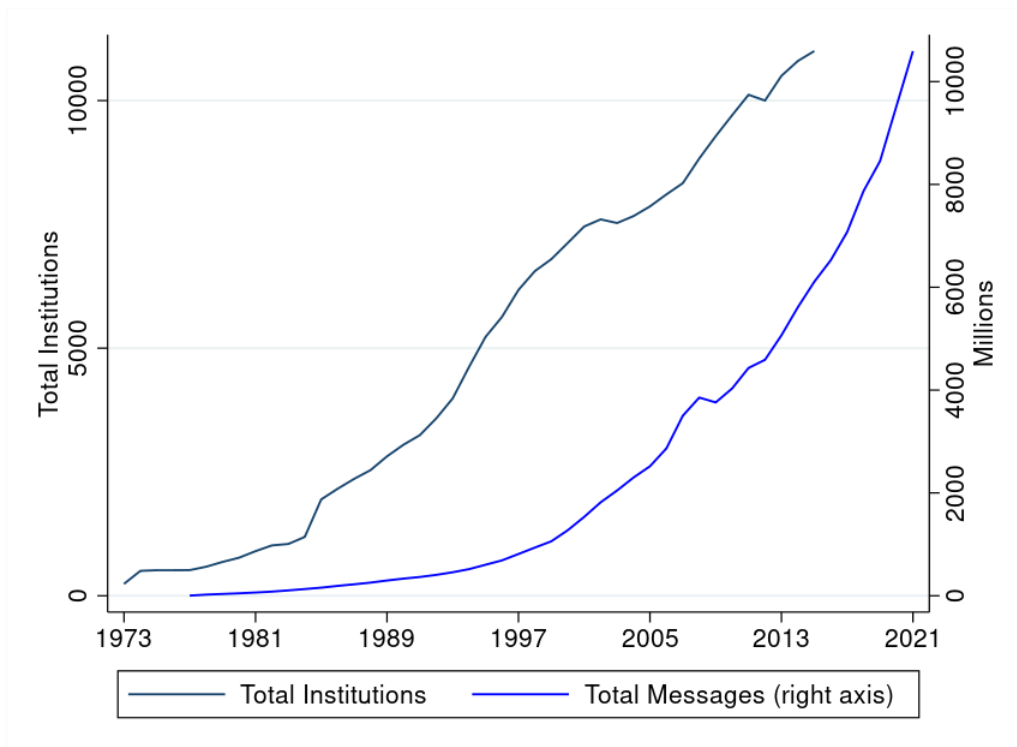


Fig. 4. Number of Institutions Connected to SWIFT and Number of SWIFT Messages

Source: authors’ calculations using data from Scott and Zachariadis (2014) and from SWIFT Annual Reviews from 2007 to 2021. The black line reports the number of institutions connected to SWIFT; the blue line reports the number of SWIFT messages (right axis).

Because SWIFT is not a payment or settlement system, the National Bank of Belgium does not regulate it as such. Since the late 1990s, however, it has been subject to the oversight of the Belgian central bank, together with the other central banks of the Group of Ten (G-10) countries and the European Central Bank, as a critical service provider. The oversight primarily focuses on the systemic risks related

to the confidentiality, integrity, and availability of the SWIFT network. In 2012, the SWIFT Oversight Forum, including an additional 15 central banks, was set up to increase information sharing on oversight activities. Because of the complexity of the SWIFT regulatory regime, the impact of central banks' oversight mainly occurs through cooperation and moral suasion.

Over the years, SWIFT has completely displaced the systems that were previously used for communicating across financial institutions and across borders; indeed, most countries have discontinued their Telex communications services in the last decade or so. In a nutshell, SWIFT has become a critical institution for international payments without any major competitors.

The Role of SWIFT in the Implementation of Financial Sanctions

SWIFT has two key roles: allowing SWIFT participants to exchange information through the SWIFT network and setting standards for messaging. International sanctions involving SWIFT prevent sanctioned entities from accessing the SWIFT network; as we discuss below, since SWIFT standards are public, sanctions cannot prevent countries from developing parallel systems that employ SWIFT standards.

Furthermore, because SWIFT is a cooperative, its mission is to act in the interest of its entire member community. As such, SWIFT typically tries not to make policy decisions that exclude users or restrict their access to the platform. Decisions to impose sanctions belong to the governments of countries, and governments around the world may (and do) impose very different sets of sanctions. As it is incorporated under Belgian law, SWIFT must comply with Belgian and EU laws and follow the sanction regimes under those jurisdictions.⁹

⁹This is explained at the SWIFT website at <https://www.swift.com/about-us/legal/compliance-0/swift-and-sanctions>.

On some occasions, SWIFT has resisted political pressure to disconnect a country from its messaging system. For instance, in 2004, SWIFT resisted the call from human rights groups to remove Myanmar from its network even after the United States and the European Union had imposed sanctions on the country. In 2014, SWIFT resisted pressure from pro-Palestinian groups to disconnect Israeli financial institutions. With these actions, SWIFT reaffirmed its commitment to function as a neutral financial service provider.

However, in February 2012, the United States passed the Iran Sanctions, Accountability, and Human Rights Act of 2012, authorizing the US president to impose sanctions on persons or institutions that provided financial messaging services to designated Iranian financial institution, including SWIFT. As a response to the US legislation, SWIFT announced the decision to discontinue access to designated Iranian financial institutions as soon as it had clarity from the European Union. On March 15, 2012, the European Union passed EU Regulation 267/2012 forbidding SWIFT from providing financial messaging services to some EU-sanctioned Iranian banks, including Iran's central bank. SWIFT complied with this regulation and disconnected the EU-sanctioned Iranian banks from its system.

The imposition of a financial sanction via SWIFT can happen without any legislative action from Belgium or the EU. In 2017, Belgium decided it would no longer allow SWIFT to provide services to certain UN-sanctioned North Korean banks, and SWIFT removed these institutions. The following week, SWIFT disconnected the remaining North Korean banks, without being required to do so by either Belgian or EU law. Although SWIFT offered an explanation for this follow-up decision by saying that the remaining banks had failed to meet its operating criteria, it did not explain what exactly the banks did that justified the suspension.

Similarly, SWIFT may decide to follow the directives of a country even if it is not required to do so by Belgian and EU law. In 2016, Iranian banks were reconnected to

SWIFT following the Joint Comprehensive Plan of Action – also known as the Iran nuclear deal of 2015 – agreed to by Iran, the United States, China, France, Russia, the United Kingdom, Germany, and the European Union. When the United States withdrew from the deal in 2018, it gave SWIFT a six-month period to disconnect the re-sanctioned Iranian institutions, or face US sanctions. Since the EU had not withdrawn from the treaty, EU regulation did not force SWIFT to disconnect the Iranian financial institutions re-sanctioned by the US. After the six-month period ended, however, SWIFT decided to disconnect the Iranian banks from its system “in the interest of the stability and integrity of the wider global financial system.” US sanctions on SWIFT would have imposed a significant impact on the global economy, given the centrality of SWIFT to the global payments system.

In 2014, following Russia’s annexation of the Crimea region of Ukraine, the United States, the European Union, and Canada introduced targeted sanctions against Russian individuals and entities, mainly travel restrictions, asset freezes, and restrictions on debt and equity financing. On September 18 2014, the European Parliament also passed a non-binding resolution (EU Resolution 2014/2841), urging EU members to exclude Russia from the SWIFT system; SWIFT objected to the resolution, reiterating its commitment to neutrality.

In February 2022, following Russia’s invasion of other areas of Ukraine, Canada, the European Union, Japan, the United Kingdom, and the United States agreed to remove some Russian (and Belarusian) banks from SWIFT, and the European Union accordingly issued EU Council Regulations 2022/345 and 398. SWIFT complied with the new EU regulation and, on March 12, 2022, it disconnected seven Russian and three Belarusian banks and their subsidiaries from its network. Three more Russian banks, one more Belarusian bank, and their subsidiaries were disconnected in June 2022.

The Emergence of SWIFT Competitors

The use of the SWIFT system as a tool for financial sanctions by the European Union, the United Kingdom, Canada, and the United States has encouraged other large countries around the world to consider building systems of their own. None of these alternatives has yet been especially successful, but their short-run goal may just be to set up a backup system both to gain expertise in the underlying technology involved and in case their access to SWIFT is threatened in the future.

In 2014, following the political pressures to disconnect Russia from SWIFT, Russia developed its own financial messaging system, SPFS (System for Transfer of Financial Messages). SPFS can transmit messages in the SWIFT format, and more broadly messages based on the ISO 20022 standard, as well as free-format messages. More than 400 banks have already connected to SPFS, most of them Russian or from former Soviet Republics. A few banks from Germany, Switzerland, France, Japan, Sweden, Turkey, and Cuba are also connected. By April 2022, the number of countries with financial institutions using SPFS had grown from 12 to 52, at which point the Central Bank of Russia decided not to publish the names of SPFS users. Due to its limited scale, SPFS mainly processes financial messages within Russia; in 2021, roughly 20 percent percent of all Russian domestic transfers were done through SPFS, with the Russian central bank aiming to increase this share to 30 percent by 2023 (Shagina, 2021).

In 2019, following Iran's loss of access to SWIFT caused by the US threat of sanctions, France, Germany, and the United Kingdom developed the Instrument in Support of Trade Exchanges (INSTEX), a special-purpose vehicle with the mission of facilitating non-SWIFT transactions with Iran. INSTEX was joined by other EU nations and made available to all member states. Although its use is limited to humanitarian purposes, it provides an example of countries setting up a parallel

system to SWIFT to side-step the threat of sanctions by another country. Note that INSTEX is not a pure messaging system, but rather a clearing house that allows payments between Europe and Iran; payments are netted within the system and direct payments between Iran and the EU happen only if there are import-export imbalances. Although the system is operational, it has been largely unused since its setup. Indeed, the first INSTEX transaction did not happen until March 2020, covering the import of medical equipment to combat the COVID-19 outbreak in Iran.

Sometimes a country decides to set up a parallel system to SWIFT for purposes that reach beyond immediate concerns over sanctions. In 2015, the People's Bank of China launched the Chinese Cross-Border Interbank Payment System (CIPS) with the purpose of supporting the use of the renminbi in international trade and international financial markets. In contrast to SWIFT, but similar to INSTEX, CIPS is not only a messaging system but also offers payment clearing and settlement services for cross-border payments in renminbi. It started with 19 direct participants and 176 indirect participants from 50 countries; at the end January 2022, there were 1,280 participants from 103 countries. Among the direct participants, eleven are foreign banks, including large banks from the United States and other developed countries. The system is overseen and backed by People's Bank of China. Similarly to Russia's SPFS, CIPS uses the SWIFT industry standard for syntax in financial messages. Indirect participants can obtain services provided by CIPS through direct participants. In 2021, CIPS processed millions of transactions for a total value of around 80 trillion yuan (\$12.7 trillion).

Several Russian banks are connected to China's CIPS as indirect participants, which facilitates Russia's business in renminbi, whereas only one Chinese bank is connected to Russia's SPFS. The presence of SPFS and CIPS allows participant institutions to interact with Russian banks, even if these banks are disconnected from SWIFT. However, although CIPS has more participants than SPFS, its overall

usage is not comparable to that of SWIFT; the CIPS payment volume is about 0.3 percent of the size of SWIFT. Most of China's CIPS transactions still actually use the SWIFT network, as many firms do not have access to a separate CIPS terminal (Yeung and Goh, 2022). Therefore, it may be hard for CIPS to become a viable substitute to the SWIFT network in the near future.

Finally, since 2001, India has developed its own secure messaging network for financial transactions, the Structured Financial Messaging System (SFMS), which allows inter- and intra-bank messaging within India. Similarly to China's CIPS and Russia's SPFS, SFMS supports the ISO 20022 standard and is therefore compatible with SWIFT. A fundamental difference is that SFMS is a purely domestic messaging system. As a result, India does not bypass SWIFT for international transactions. In October 2019, Russian, Chinese, and Indian news media reported that these countries plan to link their respective systems together (Wong and Nelson, 2021), but the extent to which this has actually happened is not clear.

The Bottom Line

Financial sanctions have often been used in international relationships, especially by Western countries, with their importance increasing over the recent decades. Sanctions that restrict access to the institutions and infrastructure supporting international payments, such as the SWIFT network, are particularly disruptive. Any kind of cross-border economic activity, be it financial or real, requires access to the international payment system. Recently, some countries have invested in creating alternative systems to allow cross-border payments without relying on institutions based in the West. While currently limited in scope, over time these alternative systems could meaningfully reduce the effectiveness of restricting access to the existing infrastructure of cross-border payments based in the West.

References

- Amicelle, Anthony.** 2011. “The Great (Data) Bank Robbery: Terrorist Finance Tracking Program and the ”SWIFT Affair”.” Technical report.
- Bank for International Settlements.** 2016. “Correspondent Banking.” Technical report, Committee on Payments and Market Infrastructures, Bank for International Settlements.
- Bank for International Settlements.** 2020. “CPMI correspondent banking chart-pack.” Technical report, BIS.
- Bech, Morten, and Jenny Hancock.** 2020. “Innovations in payments.” *BIS Quarterly Review*.
- Becker, Charles M.** 1988. “The Impact of Sanctions on South Africa and Its Periphery.” *African Studies Review*, 31(2): 61–88.
- Chang, Semoon.** 2006. “The Saga of U.S. Economic Sanctions against North Korea.” *The Journal of East Asian Affairs*, 20(2): 109–140.
- Connorton, Patrick M.** 2007. “Tracking Terrorist Financing Through SWIFT: When U.S. Subpoenas and Foreign Privacy Law Collide.” *Fordham Law Review*, 76(1): 283–322.
- Crawford, Neta C., and Audie Klotz.** eds. 1999. *How Sanctions Work Lessons from South Africa*. Houndmills: Macmillan Press LTD.
- European Commission.** 2005. “The EU’s Relations with Burma/Myanmar.” report, European Commission.
- FATF.** 2016. “Guidance on Correspondent Banking.” Technical report, Financial Action Task Force, Paris.
- Felbermayr, Gabriel, Aleksandra Kirilakha, Constantinos Syropoulos, Erdal Yalcin, and Yoto Yotov.** 2020. “The global sanctions data base.” *European Economic Review*, 129(C).
- Francioni, Francesco, and Federico Lenzerini.** 2003. “The Destruction of the Buddhas of Bamiyan and International Law.” *European Journal of International Law*, 14(4): 619–651.
- Galati, Gabriele.** 2002. “Settlement Risk in Foreign Exchange Markets and CLS Bank.” *BIS Quarterly Review*, p. 55:65.
- Ghufuran, Nasreen.** 2001. “The Taliban and the Civil War Entanglement in Afghanistan.” *Asian Survey*, 41(3): 462–487.

- Giumelli, Francesco, and Paul Ivan.** 2013. “The Effectiveness of EU Sanctions An Analysis of Iran, Belarus, Syria, and Myanmar (Burma).” Technical Report 76, European Policy Centre.
- de Goede, Marieke.** 2012. “The SWIFT Affair and the Global Politics of European Security.” *Journal of Common Market Studies*, 50(2): 214–230.
- Grolleman, Dirk, and David Jutra.** 2017. “Understanding Correspondent Banking Trends: A Monitoring Framework.” IMF Working Papers 2017/216, International Monetary Fund.
- Hardister, Angela D.** 2002. “Can We Buy a Peace on Earth: The Price of Freezing Terrorist Assets in a Post-September 11 World.” *North Carolina Journal of International Law*, 28(3): 605–661.
- Hefti, Chantal, and E. Staehelin-Witt.** 2011. “Economic Sanctions against South Africa and the Importance of Switzerland.” Technical report, Swiss National Science Foundation.
- Helwege, Ann.** 1989. “Three Socialist Experiences in Latin America: Surviving US Economic Pressure.” *Bulletin of Latin American Research*, 8(2): 211–234.
- Hufbauer, Gary Clyde, Jeffrey Schott, and Barbara Oegg.** 2001. “Using Sanctions to Fight Terrorism.” policy briefs, Institute for International Economics.
- Kirilakha, Aleksandra, Gabriel J. Felbermayr, Constantinos Syropoulos, Erdal Yalcin, and Yoto V. Yotov.** 2021. “The Global Sanctions Data Base: An Update that Includes the Years of the Trump Presidency.” In *The Research Handbook of Economic Sanctions*. ed. by Peter A.G. van Bergeijk, Cheltenham: Edward Elgar Publishing, 62–106.
- Koppel, Johannes.** 2011. *The Swift Affair*. Geneva: Graduate Institute Publications.
- Levy, Philip I.** 1999. “Sanctions on South Africa: What Did They Do?” *American Economic Association*, 89(2): 415–420.
- Livingstone, Grace.** 2009. *America’s Backyard: The United States Latin America from the Monroe Doctrine to the War on Terror*. London: Zed Books.
- Martin, Michael F.** 2012. “U.S. Sanctions on Burma.” Technical report, Congressional Research Service.
- Miller, Rena S.** 2022. “Overview of Correspondent Banking and “De-Risking” Issues.” Technical Report IF10873, Congressional Research Service.
- Olson, Richard.** 1979. “Economic Coercion in World Politics: With a Focus on North-South Relations.” *World Politics*, 31(4): 471–494.

- Petras, James, and Morris Morley.** 1975. *The United States and Chile: Imperialism and the Overthrow of the Allende Government*. New York: Monthly Review Press.
- Petras, James, and Morris Morley.** 1978. “On the U.S. and the Overthrow of Allende: A Reply to Professor Sigmund’s Criticism.” *Latin American Research Review*, 13(1): 205–221.
- Rice, Tara, Goetz von Peter, and Codruta Boar.** 2020. “On the global retreat of correspondent banks.” *BIS Quarterly Review*.
- Scott, Susan V., and Markos Zachariadis.** 2012. “Origins and Development of SWIFT, 1973-2009.” *Business History*, 54(3): 462–482.
- Scott, Susan V., and Markos Zachariadis.** 2014. *The Society for Worldwide Interbank Financial Telecommunication (SWIFT): Cooperative governance for network innovation, standards, and community*. London: Routledge.
- Sechrist, Michael.** 2010. “Cyberspace in Deep Water: Protecting Undersea Communication Cables By Creating an International Public-Private Partnership.” Technical report, Harvard Kennedy School.
- Shagina, Maria.** 2021. “How Disastrous Would Disconnection From SWIFT Be for Russia?” Carnegie Endowment for International Peace. Available at <https://carnegie.moscow.org/commentary/84634> (2021/05/28).
- Sigmund, Paul E.** 1974. “The “Invisible Blockade” and the Overthrow of Allende.” *Council on Foreign Relations*, 52(2): 322–340.
- SWIFT.** 2020. “SWIFT Annual Review: 2020.” Technical report, Society for Worldwide Interbank Financial Telecommunication.
- SWIFT.** 2021. “RMB Tracker: Monthly reporting and statistics on renminbi (RMB) progress towards becoming an international currency.” Technical report, Society for Worldwide Interbank Financial Telecommunication.
- Wong, Liana, and Rebecca M. Nelson.** 2021. “International Financial Messaging Systems.” Technical Report R46843, Congressional Research Service.
- World Bank.** 2022. “An Analysis of Trends in Cost of Remittance Services: Remittance Prices Worldwide Quarterly.” report, The World Bank Group.
- Yeung, Raymond, and Khoon Goh.** 2022. “Petroyuan Will Not Bring About a Regime Shift Soon.” Technical Report, ANZ Research.

Appendix

Table A1 shows a fictitious example of transaction involving one of SWIFT's most common messages, the MT103 message: Single Customer Credit Transfer, a type of message to convey a funds transfer instruction. When a bank sends a payment message, they include values of relevant details to each SWIFT field. Each field is associated with a Field Name which provides a brief description for the field's purpose. There are rules for each SWIFT field regarding content and format. For example, field 33A is a mandatory field specifying the value date, currency, and settled amount at the interbank level. Entries to this field must conform to the (YYMMDD)(Currency)(Amount) format.

Meaning	SWIFT Field	Value
Sender	Block1/LTabB1	BXYZCHZZ80A
Message type	Block2/Msgtype	103
Receiver	Block2/LTabB2	BNPSFRZA93B
Uniq. ETE Tr. Ref.	121	1234-ABCD-9876-XYZA-a...
Sender's Reference	20	1234ABCD...
Bank Operation Code	23B	CRED
Interbank sett. Mnt.	32A	180724EUR500000,
Currency / Instr. Mnt	33B	EUR499950,0
Ordering Customer	50K	/CH5704835098735711000 Robert Lewis ...
Beneficiary customer	59	/FR7630004008180001236 Evergreen SARL ...

Table A1. Fictitious example of SWIFT payment message with explanation of different fields.

The Sender Bank is notifying the Receiver Bank of a funds transfer on behalf of the Sender's client, Robert Lewis, to be delivered to the Receiver's client, Evergreen SARL.