SWIFT as an example of Cross-Border Settlement Systems

by

Alejandro Sosa

Unclassified Topic Paper, submitted to the faculty of the National Intelligence University in partial fulfillment of the requirements for MST 682, Cyber Intelligence.

31 October 2023

The views expressed in this paper are those of the author and do not reflect the official policy or position of the Department of Defense, US Air Force, or the US Government

Across all forms of governance, politics, and religion, there is at least one thing upon which all systems today rely. Finances are the cornerstone of modern society. Without a properly functional international financial system, everything would become much more difficult, especially given the hyperspecialized nature of the modern global economy where goods are often initially built in one area from raw material from another nation and finally finished in yet another nation. The world has increased in complexity by orders of magnitude. At the heart of that industry are banks that communicate and trade funds to ensure that an international seller on Amazon receives the funds from an American Express card, paid by a regional credit union. Especially in a digital economy where physical currency never changes hands, people, businesses, governments, and banks rely upon financial messaging systems like SWIFT in order to settle transactions. The ubiquity of these cross-border payment systems, specifically SWIFT, has made them such valuable tools in targeting sanctions[1].

Cross-border payments tend to be incredibly complex. I will give a brief overview of what settlement systems look like to underscore the level of communication that must occur and the sheer number of actors involved. Often, due to the high number of transactions and the total volume of money involved across all transactions, many governmental central banks have set up "real-time gross settlement" systems that allow the settlement of payments in real-time, on a gross basis. An example of this is wiring money in the US. If X wants to send money to Y, then X's bank's account balance with the central bank will decrease, and Y's bank's account balance with the central bank will increase in proportion, and money will flow from and to those individual's respective banks accounts from the bank's accounts with the central bank. If this sounds complex, remember that this is before money has to be converted from one currency to

[1] Marco Cipriani, Linda S. Goldberg, and Gabriele La Spada, "Financial Sanctions, SWIFT, and the Architecture of the International Payment System," *Journal of Economic Perspectives* 37, no. 1 (February 2023): 31–52, https://doi.org/10.1257/jep.37.1.31.

another and does not involve third- or fourth-party payment companies yet. See Graphic 1 for a visual representation of this system.

Prior to the development of SWIFT messaging, banks communicated nationally and internationally using Telex systems. Telex systems ran over telegraph and telephone networks, allowing speech and rudimentary analog data over the same connection. This system was costly and insecure. There had to be independent authorizations set up between each node, and each transaction took ten or more messages. In the 1970s, Citibank developed a proprietary messaging system called MARTI (Machine Readable Telegraphic Input). Citibank tried to force adoption onto partner banks both in the United States and Europe. Rather than be coerced into a perceived US-owned system, 239 banks from 15 countries founded the Society for Worldwide Interbank Financial Telecommunication[2]. It is headquartered in Belgium and organized as a cooperative. Today, the primary role of SWIFT messaging in international banking is to securely transport messages containing payment instructions between financial institutions conducting business, as illustrated in Graphic 2. SWIFT can also offer a secure person-to-person messaging network for the transfer of invoices and contracts. SWIFT is not an escrow system; it does not hold any money; it is solely a messaging service. SWIFT has become a critical service in cross-border settlement systems. Studies have shown that due to efficiencies gained by using SWIFT, it has led to an increase in profitability in the long term, especially for smaller banks, allowing them greater participation in international markets with relatively low costs[3]. Yet that has not stopped hackers from attacking the system in order to steal money from banks.

[2] Susan V. Scott and Markos Zachariadis, "Origins and Development of SWIFT, 1973–2009," *Business History* 54, no. 3 (June 1, 2012): 462–82, https://doi.org/10.1080/00076791.2011.638502.

[3] Susan V. Scott, John Van Reenen, and Markos Zachariadis, "The Long-Term Effect of Digital Innovation on Bank Performance: An Empirical Study of SWIFT Adoption in Financial Services," *Research Policy* 46, no. 5 (June 1, 2017): 984–1004, https://doi.org/10.1016/j.respol.2017.03.010.

There are a handful of high-profile incidents of hackers utilizing the SWIFT messaging service to steal money from central banks. The most visible and broadly reported incident involved hackers targeting the central bank of Bangladesh. Hackers employed a malware known as Dridex, which was activated when victims who were likely spear-phished opened fraudulent Microsoft Word or Excel attachments from spurious e-mails. The hackers utilized key loggers in order to obtain the credentials required to make fraudulent transactions.[4] It is estimated that between $80-$100M dollars were stolen, although some of the money was later recovered.

Despite this high-profile attack, the SWIFT system is still considered to be incredibly safe. This may be because, ultimately, previous thefts have not been due to flaws in the messaging service or network but due to human compromise of credentials.[5] SWIFT offers two key roles to the global financial community, both the messaging service that it runs and the standardization of financial messaging formats for the industry. Currently, there are nine broad categories of SWIFT messages, including foreign exchange transactions and simple fund transfers. SWIFT constantly develops new message standard formats that dramatically facilitate financial transactions worldwide. SWIFT has developed specific Business Identifier Codes (BIC), International Bank Account Numbers (IBAN), and codes for exchange and market identification.[6]

GRAPHIC 1[7]

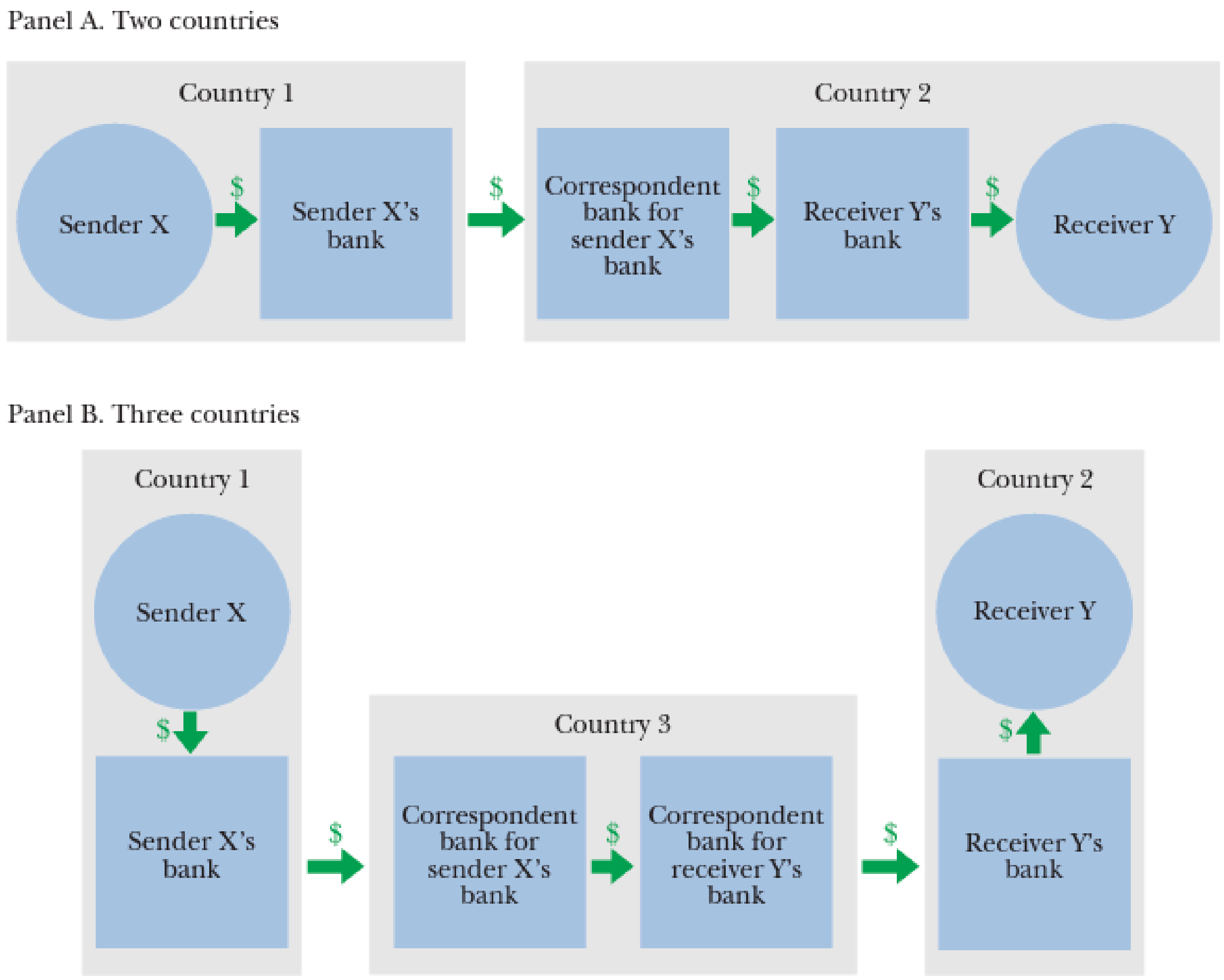
[4] John Harvey, "The Financial Sector's Vulnerabilities, Villains, and Options for Defense," *Military Cyber Affairs* 3, no. 2 (February 18, 2019), https://doi.org/10.5038/2378-0789.3.2.1062.

[5] Elizabeth Petrie and Casey Evans, "Sharing Insider Threat Indicators: Examining the Potential Use of Swift's Messaging Platform to Combat Cyber Fraud," SSRN Scholarly Paper (Rochester, NY, October 2, 2017), https://papers.ssrn.com/abstract=3047777.

[6] Cipriani, Goldberg, and La Spada, "Financial Sanctions, SWIFT, and the Architecture of the International Payment System."

[7] Cipriani, Goldberg, and La Spada.

Cross-border Payments and Correspondent Banking



Panel A. Two countries

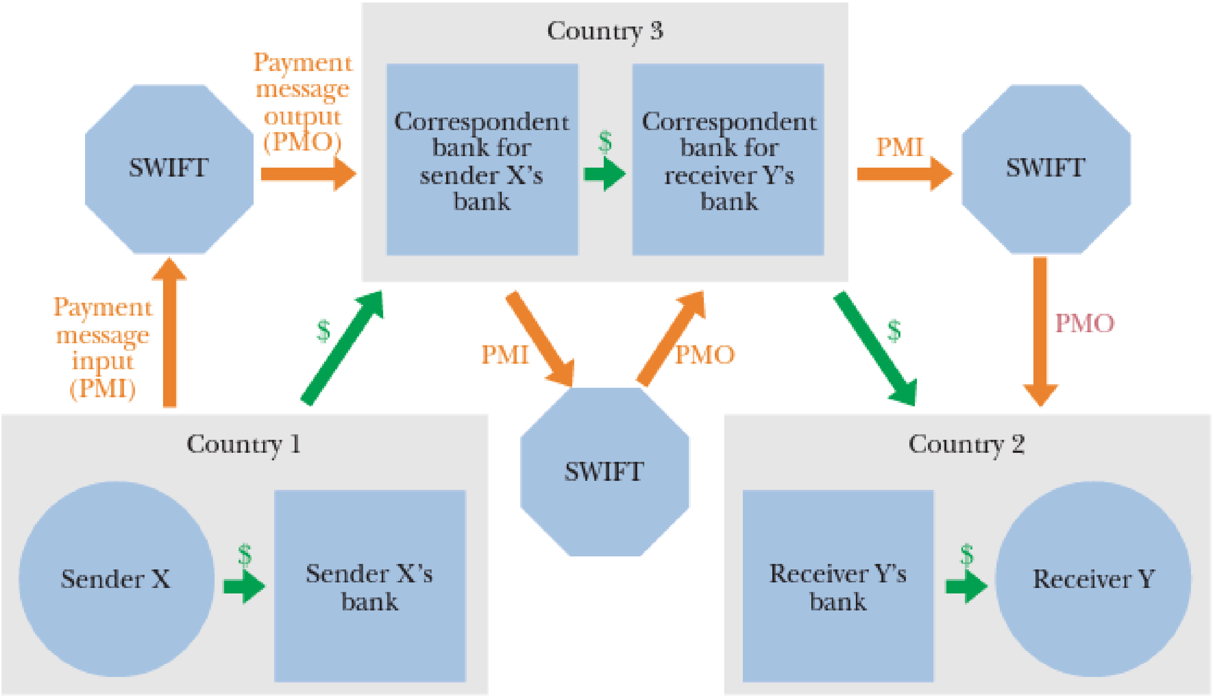
Panel B. Three countries

Source: Authors' construction.
Note: 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.

GRAPHIC 2[8]

[8] Cipriani, Goldberg, and La Spada.

The Role of SWIFT in Cross-border Payments


Country 3
Correspondent bank for sender X's bank
$
Correspondent bank for receiver Y's bank
Payment message output (PMO)
SWIFT
PMI
SWIFT
Payment message input (PMI)
$
PMI
PMO
$
PMO
Country 1
Sender X
$
Sender X's bank
SWIFT
Country 2
Receiver Y's bank
$
Receiver Y

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

Works Cited

Cipriani, Marco, Linda S. Goldberg, and Gabriele La Spada. “Financial Sanctions, SWIFT, and the Architecture of the International Payment System.” *Journal of Economic Perspectives* 37, no. 1 (February 2023): 31–52. https://doi.org/10.1257/jep.37.1.31.

Harvey, John. “The Financial Sector’s Vulnerabilities, Villains, and Options for Defense.” *Military Cyber Affairs* 3, no. 2 (February 18, 2019). https://doi.org/10.5038/2378-0789.3.2.1062.

Petrie, Elizabeth, and Casey Evans. “Sharing Insider Threat Indicators: Examining the Potential Use of Swift’s Messaging Platform to Combat Cyber Fraud.” SSRN Scholarly Paper. Rochester, NY, October 2, 2017. https://papers.ssrn.com/abstract=3047777.

Scott, Susan V., John Van Reenen, and Markos Zachariadis. “The Long-Term Effect of Digital Innovation on Bank Performance: An Empirical Study of SWIFT Adoption in Financial Services.” *Research Policy* 46, no. 5 (June 1, 2017): 984–1004. https://doi.org/10.1016/j.respol.2017.03.010.

Scott, Susan V., and Markos Zachariadis. “Origins and Development of SWIFT, 1973–2009.” *Business History* 54, no. 3 (June 1, 2012): 462–82. https://doi.org/10.1080/00076791.2011.638502.