SWIFT Bank Heists and Article 4A

Julie Andersen Hill

JOURNAL OF CONSUMER AND COMMERCIAL LAW
Volume 22, No. 1, Pages 25-30 (2018)

SWIFT Bank Heists and Article 4A

By Julie Andersen Hill•

The days when an enterprising bank robber could make a living with a ski mask and pistol are over. Thanks to security protocols implemented by banks, the typical bank hold-up nets only about $6,500 dollars.[1] Moreover, the FBI is incredibly good at tracking down these criminals. About half of these bank robbers are eventually identified by the FBI.[2]

But a new breed of bank robber has emerged. Computer hackers are capable of anonymously stealing billions of dollars through fraudulent wire transfers. Banks in Ecuador, Bangladesh, Vietnam, Nepal, India, Russia, and elsewhere have been attacked.[3]

When law enforcement is unsuccessful in tracking down the hackers, parties to the fraudulent transactions turn to the law to determine who must bear the loss. In the United States, responsibility for fraudulent wire transfers is governed by Article 4A of the Uniform Commercial Code. Because wire transfers are often routed through the United States or transferred pursuant to contracts with U.S. choice of law provisions, Article 4A will ultimately apportion the loss of at least some international cyber bank heists. This article explains how Article 4A works by considering the facts of a 2016 heist at Bangladesh Bank.[4]

I. The Bangladesh Bank Heist

In 2016, hackers infiltrated the computers at Bangladesh Bank, the central bank of the country of Bangladesh.[5] The hackers instructed the Federal Reserve Bank of New York ("New York Fed") to wire nearly $1 billion dollars from Bangladesh Bank's account to accounts in Sri Lanka and the Philippines.[6] Some of the payment orders were stopped, but $81 million in fraudulent wires were processed and lost.[7]

A. The Infiltration

The point of attack was the SWIFT system at Bangladesh Bank.[8] SWIFT (Society for Worldwide Interbank Financial Telecommunications) is a bank-to-bank electronic messaging system that is the primary means for communicating international wire transfers.[9] SWIFT processes billions of wire transfers every year.[10]

It is not clear exactly how the hackers got access to the SWIFT system at Bangladesh Bank. Some have suggested the hackers likely sent a scam e-mail to an employee at the bank. When the employee opened the e-mail, it installed a virus. The virus recorded keystrokes and captured passwords.[11] Other sources speculate that Bangladesh Bank employees may have intentionally compromised the computer system.[12]

At any rate, computer security was lax. The computers running the SWIFT system were connecting to the internet and had no firewall. In what might be considered the understatement of the year, one Bangladesh Bank official said: "There might have been a deficiency in the system in the SWIFT room."[13]

Once in the system, hackers installed software that would bypass some of the security features in SWIFT and make it more difficult for the bank to discover the theft. For example, the malware prevented the printer from automatically printing a copy of outgoing payment orders. [14]

B. The Attack

After installing the malware, the thieves waited until the bank closed for the day on Thursday, February 4, 2016 to attack. Then they logged onto the Bangladesh Bank system and begin sending payment orders – thirty-five in all. They instructed the New York Fed to send money from Bangladesh Bank's account there, to banks in other countries. The payment orders totaled nearly $1 billion.[15]

The New York Fed flagged thirty of the payment orders because it needed more information to confirm that the orders did not implicate sanctioned countries or people.[16] The New York Fed began sending messages to the Bangladesh Bank for clarification on these orders. However, the New York Fed had already processed five orders when it discovered the red flags and began investigating the payment orders.[17]

Once in the system, hackers installed software that would bypass some of the security features in SWIFT and make it more difficult for the bank to discover the theft.

One of the orders that went through sent $20 million to Pan Asian Bank in Sri Lanka. The Sri Lankan bank thought the payment seemed unusually large for a country the size of Sri Lanka. It also noticed that the name of the account holder appeared to be misspelled – it said "Fandation" instead of "Foundation." Pan Asian Bank held the funds while it checked with a correspondent bank to confirm that it had received the order correctly. This delay meant that Bangladesh Bank was ultimately able to recover the $20 million sent through that order.[18]

The other four orders, however, were successfully sent to Rizal Commercial Banking Corporation ("RCBC") in the Philippines.[19]

C. The Getaway

At RCBC, the money was deposited into accounts that had been set up with fake names and fake addresses. From the bank, the money was stuffed into bags and transferred to Philippine casinos. There "high rollers" gambled the money playing baccarat. This method of money laundering was effective. Investigators have been unable to trace the money any farther than the casinos. [20]

D. The Discovery

Meanwhile, bank officials were slow to notice and respond to the theft. The theft seems to have been timed to coincide with the weekend in Bangladesh. On Friday, an employee arrived at Bangladesh Bank and noticed no payment orders had printed. When he was unable to get the orders to print, he asked someone else to fix the printer, and he went home.[21]

On Saturday, the employee returned to Bangladesh Bank to find that the printer still was not working. This time when he tried to log onto the SWIFT system, he got an error message. Bangladesh Bank employees worked to fix the software. A few hours later they got the orders to print out and realized that something horrible had happened.[22]

With their SWIFT system not working, Bangladesh Bank employees looked for a way to contact the New York Fed. They found an e-mail address online and sent three messages stating that their account had been hacked. But that e-mail address at the Fed was not monitored on the weekend. They also called and sent a fax, but those communication channels similarly were not monitored over the weekend.[23]

By Monday the New York Fed was open and Bangladesh Bank had its SWIFT system operational again. Bangladesh Bank sent more than 100 SWIFT messages to RCBC in the Philippines,[24] but RCBC was closed because it was the Chinese New Year. By the time RCBC finally acted, the money was gone.[25]

II. Who Bears the Loss?

Who will bear this $81 million dollar loss? If the thieves and the money could be located they would be responsible for the crime. But the chances of catching the mastermind behind this attack seem slim and the chances of recovering the money even slimmer. Authorities suspect the North Korean government was ultimately responsible for the theft.[26]

The question then becomes who among the banks will bear the loss for the theft. The possibilities include:

- Bangladesh Bank – the purported "originator"[27] and "sender"[28] of the payment orders.
- The Federal Reserve Bank of New York – the "receiving bank" because it received the payment orders purportedly from Bangladesh Bank.[29]
- Rizal Commercial Bank Corporation in the Philippines – the "beneficiary's bank."[30]

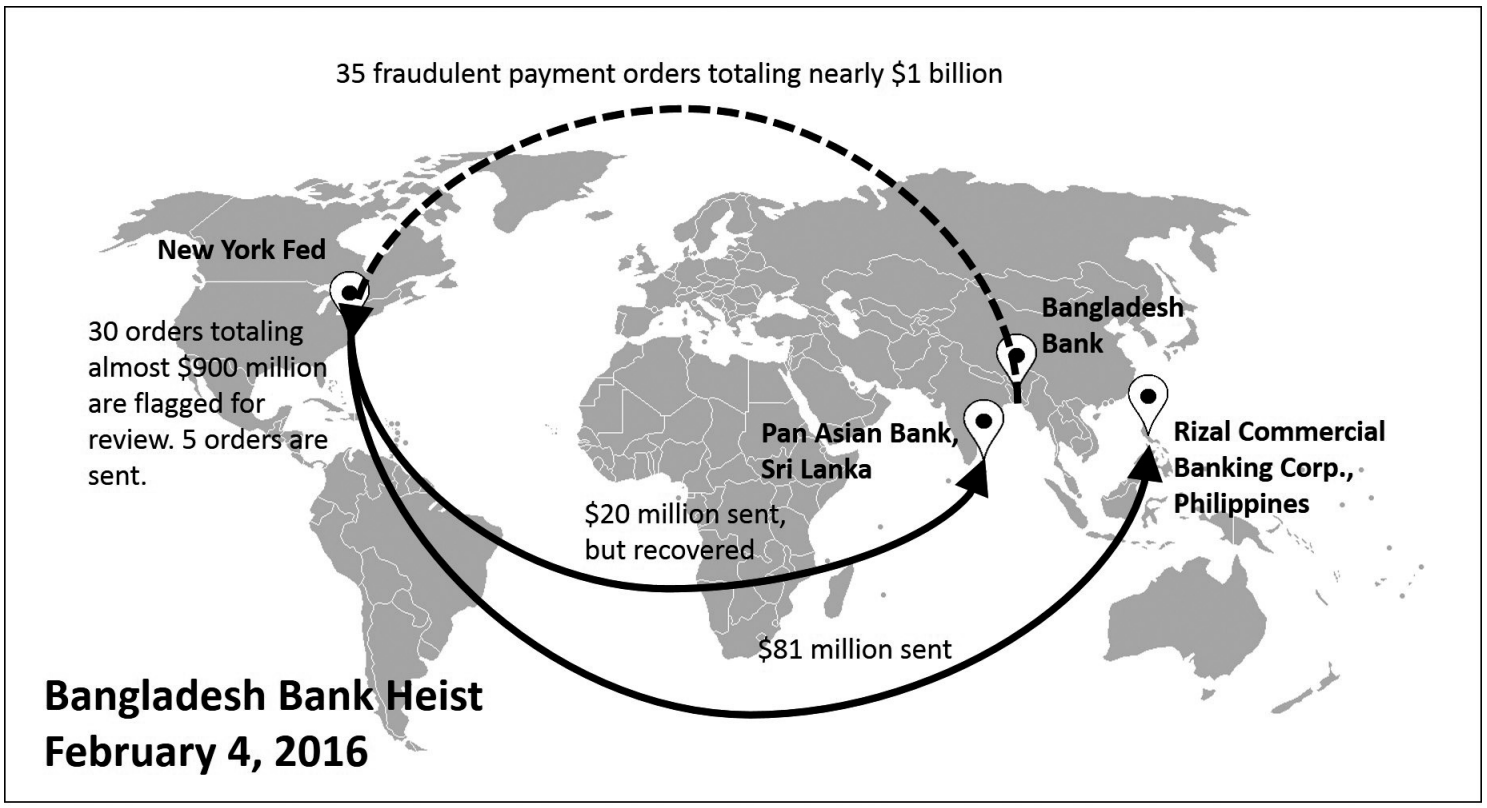
Deciding what law applies to multi-bank, multi-country wire transfers can be tricky.[31] There is, however, reason to believe U.S. law may apply in this and other similar cases. Here the money was sent from a bank in the United States. In addition, Bangladesh Bank signed an agreement with the New York Fed that likely provided that New York law governs wires from its account.[32] New York, like all U.S. states, has adopted Article 4A of the Uniform Commercial Code. [33]

A. The Receiving Bank

Initially, Bangladesh Bank announced that it planned to sue the New York Fed for processing the fraudulent payment orders.[34] The UCC rule for apportioning loss between a sender (here Bangladesh Bank) and a receiving bank (the New York Fed) provides:

> If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether or not authorized, if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer. . . .[35]

Assuming Bangladesh Bank signed the standard agreement with the New York Fed, the Bank agreed to authentication of payment orders through SWIFT alone.[36] SWIFT authentication meets the



requirements of a security procedure.[37] This leaves two questions. First, is SWIFT authentication alone a "commercially reasonable" security procedure? Second, did the New York Fed act in "good faith" and in compliance with the security procedure?

1. Commercially Reasonable

Whether a security procedure is commercially reasonable is a question of law.[38] In deciding the question, a court should consider "the wishes of the customer . . . , the circumstances of the customer . . ., including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated."[39]

One recent case considered whether SWIFT authentication alone was commercially reasonable under the UCC.[40] There hackers gained access to the SWIFT system of a bank in Ecuador. The hackers instructed Wells Fargo Bank to transfer $12 million from the Ecuadorian bank's account at Wells Fargo to various accounts in Hong Kong, Dubai, and elsewhere.[41] The Ecuadorian bank sued Wells Fargo in federal court in New York alleging that it was not commercially reasonable for Wells Fargo to authenticate the wires with SWIFT only.[42] Wells Fargo asked the court to dismiss the case for failure to state a claim.[43] The court did not dismiss the case noting the "fact-intensive nature of the commercial reasonableness inquiry."[44] Thus, the court left open the possibility that SWIFT authentication could be commercially unreasonable. But we do not know what the court would have decided if it had reached the merits of the claim. The parties reached a confidential settlement dismissing the case.[45]

If a court were to conclude that SWIFT alone is not a commercially reasonable method of providing security against unauthorized payment orders, the decision would have widespread ramifications. "The vast majority of both commercial banks and central banks around the world rely on SWIFT's secure communication channel and authentication protocols as their primary method of verifying the banking instructions received from counterparties are authentic."[46] Adding additional security procedures would be costly and would increase the time it takes to process payments. Senders of payment orders are unlikely to welcome the idea of slower, more expensive wire transfers.

For example, after the Bangladesh Bank heist, the New York Fed and Bangladesh Bank implemented additional security protocols including voice authentication to confirm authorization of payments. "Fed officials had to call one or two or three Bangladesh Bank officials whose voice samples were shared with the Fed."[47] Bangladesh Bank found the process "delayed genuine transfer instructions."[48] To free itself from the cumbersome process, Bangladesh Bank improved the security of its computers so it could once again send payments authenticated solely by SWIFT.[49]

This return to SWIFT authentication probably explains why Bangladesh Bank seems to have abandoned the idea of suing the New York Fed. It would seem inconsistent for the Bank to argue in court that SWIFT authentication is insufficient, after persuading the Fed to return to the practice of using only SWIFT authentication. [50]

2. Good Faith

The remaining question under UCC Article 4A-202 is whether the New York Fed "accepted the payment order in good faith and in compliance with the security procedure."[51] Good faith under the UCC means "honesty in fact and observance of reasonable commercial standards of fair dealing."[52] In the Bangladesh Bank heist case, the New York Fed followed the SWIFT authentication protocols[53] and there have been no press reports that the New York Fed was not honest. Thus, the question under the good faith prong of 4A-202 is whether the New York Fed followed reasonable commercial standards in processing the transactions.

This is technically a different question than the previously addressed question of whether the security procedure itself was commercially reasonable.[54] As the United States Court of Ap-

peals for the Eighth Circuit has explained:

> While the commercial reasonableness inquiry concerns the adequacy of a bank's security procedures, the objective good faith inquiry concerns a bank's acceptance of payment orders in accordance with those security procedures. In other words, technical compliance with a security procedure is not enough under Article 4A; instead, as the above-quoted materials indicate, the bank must abide by its procedures in a way that reflects the parties' reasonable expectations as to how those procedures will operate.[55]

Nevertheless, in cases where the receiving bank's authorization protocol is automated[56] and "there is no plausible allegation that the authorizing bank failed to adhere to the agreed-upon security procedure . . .[,] the two inquiries largely collapse."[57] Because the SWIFT system is largely automated, in most cases resulting from a hack into the sender's SWIFT system, the receiving bank will be able to show that it acted in good faith. This may be another reason Bangladesh Bank ultimately decided not to sue the New York Fed.[58]

B. The Beneficiary Bank

Bangladesh Bank, however, is still exploring its claims against the Philippine bank RCBC. Bangladesh Bank has threatened to sue RCBC in the United States[59] and is reportedly considering an out-of-court settlement.[60] RCBC has repeatedly denied any responsibility to Bangladesh Bank,[61] but it may also be contemplating a settlement.[62] The main point of contention appears to be whether RCBC should have cancelled the payment orders before allowing the thieves to withdraw the money from the bank.[63]

Under the UCC "a communication by the sender cancelling . . . a payment order is effective to cancel . . . the order if notice of the communication is received at a time and in a manner affording the receiving bank a reasonable opportunity to act on the communication before the bank accepts the payment order."[64] If, however, the receiving bank has already accepted a payment order, "cancellation . . . is not effective unless the receiving bank agrees."[65]

Delayed detection often means the money will have disappeared forever.

Thus the preliminary question is whether the beneficiary bank accepted the payment order before the order was cancelled. Under the UCC, there are several ways that a beneficiary bank can accept a payment order. For example, a beneficiary bank accepts the order when "(i) the beneficiary is notified of the right to withdraw the credit, (ii) the bank lawfully applies the credit to a debt of the beneficiary, or (iii) funds with respect to the order are otherwise made available to the beneficiary by the bank." [66]

Press reports in the Bangladesh Bank heist leave some question as to whether RCBC received the cancellation orders in enough time to act before it accepted the orders. Although money was withdrawn from RCBC on Tuesday, it could have been in the beneficiary accounts and available for withdrawal on Monday or before. It is also difficult to determine when RCBC can be deemed to have received requests to cancel the payment. RCBC was closed on Monday and the messages it received on Tuesday were not sent as urgent. RCBC claims its employees did not read the orders until after the money had already been withdrawn.[67]

If a court found that RCBC received the cancellation messages in enough time to act before accepting the orders, then RCBC would be responsible for the loss under the UCC. If, however, RCBC had already accepted the payment orders, RCBC would have to agree to cancel the wires.

If RCBC had already accepted the payment orders, it is not hard to see why it did not agree to cancel the orders. Under the UCC, if a beneficiary bank agrees to cancel an order, the beneficiary bank can recover the money from the beneficiary "to the extent allowed by the law governing mistake and restitution."[68] Of course, to recover from the beneficiary, RCBC would have to find the beneficiary and the money. So far the best law enforcement on two continents has been unsuccessfully in tracking down the thieves or the money. Most banks would not want to sign up for that task.

III. Conclusion

In sum, it is unlikely that UCC Article 4A will help most originators who find their SWIFT systems have been hacked. Originators of payment orders should carefully consider security procedures used to authenticate payment orders. If an originator agrees to a payment order, it may be an uphill battle to later convince a court that the agreed upon procedure was commercially unreasonable. Originators should also vigilantly watch for evidence that their payment systems may have been compromised. If fraudulent orders are detected early, the originator may be able to cancel the order and recover the money. Delayed detection often means the money will have disappeared forever.

* ©*Julie Andersen Hill, Alton C. and Cecile Cunningham Craig Professor of Law, University of Alabama.*

---

1 Justin Jouvenal, *A Quintessentially American Crime Declines: Robbing Banks Doesn't Pay as It Used To*, Wash. Post, Oct. 6, 2016, *available at* 2016 WLNR 30691475.

2 U.S. Dep't of Just. & Fed. Bureau of Investigation, Bank Crime Statistics (2016), *available at* https://www.fbi.gov/file-repository/bank-crime-statistics-2016.pdf/view.

3 *See* Tom Bergin & Jim Finkle, *SWIFT Confirms New Cyber Thefts, Hacking Tactics*, Reuters, Dec. 12, 2016, https://www.reuters.com/article/us-usa-cyber-swift-exclusive-idUSKBN1412NT (Bangladesh, Ecuador, and Vietnam); Gopal Sharma, *Nepal Recovers "Most" of the Money Hacked from Bank*, Reuters, Nov. 7, 2017, https://www.reuters.com/article/us-cyber-heist-nepal/nepal-recovers-most-of-the-money-hacked-from-bank-idUSKBN1D72JP; Devidutta Tripathy, *India's City Union Bank Says Suffered Cyber Hack Via SWIFT System*, Reuters, Feb. 18, 2018, https://www.reuters.com/article/us-city-union-bank-swift/indias-city-union-bank-ceo-says-suffered-cyber-hack-via-swift-system-idUSKCN1G20AF; Jack Stubbs, *Hackers Stole $6 Million from Russian Bank Via SWIFT System: Central Bank*, Reuters, Feb. 16, 2018, https://www.reuters.com/article/us-russia-cyber-swift/hackers-stole-6-million-from-russian-bank-via-swift-system-central-bank-idUSKCN1G00DV; Joshua Hammer, *The Billion-Dollar Bank Job*, N.Y Times, May 6, 2018, at MM43 (stating that banks in Taiwan and Poland had also been targeted by cyber attacks).

4 This article is not meant as a definitive evaluation of legal liability for the Bangladesh Bank heist. Because investigations into the heist are still ongoing and no claims have been litigated, determining liability now would premature. This article seeks only to use publicly released information about the Bangladesh Bank heist to illustrate the operation of UCC Article 4A.

5 Hammer, *supra* note 3.

6 Raju Gopalakrishnan & Manuel Mogato, B*angladesh Bank Of-*

ficial's Computer Was Hacked to Carry Out $81 Million Heist: Diplomat, Reuters, May 19, 2016, https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-officials-computer-was-hacked-to-carry-out-81-million-heist-diplomat-idUSKCN0YA0CH.

7 *Id*.

8 Jim Finkle, *Bangladesh Bank Hackers Compromised SWIFT Software, Warning Issued*, Reuters, Apr. 25, 2016, https://www.reuters.com/article/us-usa-nyfed-bangladesh-malware-exclusiv/bangladesh-bank-hackers-compromised-swift-software-warning-issued-idUSKCN0XM0DR.

9 Ronald J. Mann, Payment Systems and Other Financial Transactions 213 (6th ed. 2016)("SWIFT (the Society for Worldwide Interbank Financial Telecommunications) is an automated international system for sending funds-transfer messages that is the predominant method for completing international transfers that are not denominated in dollars.").

10 SWIFT, Annual Review 4 (2017), *available at* https://www.swift.com/file/51966/download?token=0UogFJo6.

11 Chelsea Allison, *Anatomy of a Bank Heist*, FIN, June 1, 2018, https://fin.plaid.com/articles/anatomy-of-a-bank-heist; Victor Mallet & Avantika Chilkoti, *How Cyber Criminals Targeted Almost $1bn in Bangladesh Bank Heist*, Fin. Times, Mar. 18, 2016, https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8.

12 Devlin Barrett & Kate O'Keeffe, *FBI Suspects Insider Involvement in $82 Million Bangladesh Central-Bank Heist*, Wall St. J., May 11, 2016, at C1.

13 Serajul Quadir, *Malware Suspected in Bangladesh Bank Heist: Officials*, Reuters, Mar. 11, 2016, https://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0XI1UO.

14 Finkle, *supra* note 8 (noting that the software could also "manipulate account balances on logs to prevent the heist from being discovered until after the funds had been laundered").

15 Krishna N. Das & Jonathan Spicer, *How the New York Fed Fumbled Over the Bangladesh Bank Cyber-Heist*, Reuters, July 21, 2016, https://www.reuters.com/investigates/special-report/cyber-heist-federal/.

16 *Id*. (noting that the "Jupiter" name of the Philippine bank branch raised a red flag because an unrelated oil tanker named Jupiter was under trade sanctions with Iran).

17 Letter from Thomas C. Baxter, Jr., Gen. Couns. and Executive V.P., Fed. Res. Bank of New York, to Carolyn B. Maloney, Representative, U.S. Congress, Apr. 14, 2016 [hereinafter Baxter Letter] (discussing the 30 orders held for further investigation).

18 Serajul Quadir, *How a Hacker's Typo Helped Stop a Billion Dollar Bank Heist*, Reuters, Mar. 10, 2016, https://www.reuters.com/article/us-usa-fed-bangladesh-typo-insight/how-a-hackers-typo-helped-stop-a-billion-dollar-bank-heist-idUSKCN0WC0TC.

19 Hammer, *supra* note 3.

20 *See id*.; Alan Katz & Wenxin Fan, *A Baccarat Binge Helped Launder the World's Biggest Cyberheist*, Bloomberg, Aug. 3, 2017, https://www.bloomberg.com/news/features/2017-08-03/a-baccarat-binge-helped-launder-the-world-s-biggest-cyberheist.

21 *See* Das & Spicer, *supra* note 15.

22 *See id*.

23 *See id*.

24 *See* Allison, *supra* note 11.

25 *See* Krishna N. Das & Jonathan Spicer, *How Millions from the Bangladesh Bank Heist Disappeared*, Reuters, July 21, 2016, https://www.reuters.com/article/us-cyber-heist-philippines/how-millions-from-the-bangladesh-bank-heist-disappeared-idUSKCN1011AT.

26 Karen Lema, *Bangladesh Bank Heist Was "State-Sponsored": U.S. Official*, Reuters, Mar. 29, 2017, https://www.reuters.com/article/cyber-heist-philippines/bangladesh-bank-heist-was-state-sponsored-u-s-official-idUSL2N1H61ZH.

27 U.C.C. § 4A-104(c) (Am. Law Inst. & Unif. Law Comm'n 2012) ("'Originator' means the sender of the first payment order in a funds transfer.").

28 *Id*. § 4A-103(a)(5) ("'Sender' means the person giving the instruction to the receiving bank.").

29 *Id*. § 4A-103(a)(4) ("'Receiving bank' means the bank to which the sender's instruction is addressed."). The Federal Reserve is also the "'[o]riginator's bank' mean[ing] . . . the receiving bank to which the payment order of the originator is issued [when] the originator is not a bank.").

30 *Id*. § 4A-103(a)(3) ("'Beneficiary's bank' means the bank identified in a payment order in which an account of the beneficiary is to be credited pursuant to the order or which otherwise is to make payment to the beneficiary if the order does not provide for payment to an account.").

31 *See generally* John S. Santa Lucia, Comment, *Exchange Losses from International Electronic Funds Transfers: Time to Unify the Law*, 8 Nw. J. Int'l L & Bus. 759 (1988) (noting that SWIFT transfers are not subject to any international law).

32 In response to a Freedom of Information Act request, the New York Fed released its "standard account agreement template for accounts maintained at the New York Fed for foreign central banks and monetary authorities." Statement, Fed. Res. Bank of New York, New York Fed Responds to Freedom of Information Request (Aug. 11, 2016), *available at* https://www.newyorkfed.org/newsevents/statements/2016/foia-cbias. The agreement states:

> Notwithstanding any other provision of this Agreement, the Reserve Bank is only liable for acting on an unauthorized funds transfer instruction if the Reserve Bank fails to comply with the agreed-upon security procedure used to authenticate such instruction or, when acting on such instruction, fails to act under principles of good faith as defined in Article 4A of the Uniform Commercial Code of the State of New York.

Account Agreement Between the Federal Reserve Bank of New York and [Name of Organization] (Aug. 11, 2016), *available at* https://www.newyorkfed.org/medialibrary/media/newsevents/statements/2016/foia-cbias.pdf [hereinafter Standard Foreign Central Bank Contract]. The agreement further provides that "the rights and obligations described herein or arising out of this Agreement will be governed by the Federal law of the United States of America and, in the absence of controlling Federal law, in accordance with the laws of the State of New York." *Id*.

33 Kathleen Patchel, et al., *The Uniform Commercial Code Survey: Introduction*, 54 Bus. Law. 1827, 1829 (1999).

34 Serajul Quadir, *Bangladesh Bank Weighs Lawsuit Against NY Fed Over Hack*, Reuters, Mar. 22, 2016, https://www.reuters.com/article/us-usa-fed-bangladesh/bangladesh-central-bank-weighs-lawsuit-against-ny-fed-over-cyber-heist-idUSKCN0WO2JQ.

35 U.C.C. § 4A-202(b).

36 The standard agreement states that the account holder agrees to use "the S.W.I.F.T. authentication protocols then in effect or, if applicable, the other authentication procedures specified in the Terms of Service as a security procedure for the authentication of payment or other instructions." Standard Foreign Central Bank Contract, *supra* note 32. There are no indications that Bangladesh Bank had agreed to other security procedures through a separate Terms of Service agreement.

37 U.C.C. § 4A-201 ("'Security procedure' means a procedure established by agreement of a customer and a receiving bank for

the purpose of . . . verifying that a payment order or communication amending or cancelling a payment order is that of the customer . . . .").

38 *Id*. § 4A-202(c).

39 *Id*.

40 Banco del Austro, S.A. v. Wells Fargo Bank, N.A., 215 F. Supp. 3d 302 (S.D.N.Y. 2016).

41 Clare Baldwin & Nathan Layne, *In Ecuador Cyber Heist, Thieves Moved $9 Million to 23 Hong Kong Firms*, Reuters, May 25, 2016, https://www.reuters.com/article/us-cyber-heist-hongkong-exclusive-idUSKCN0YG2W9; Tom Bergin & Nathan Layne, *Special Report: Cyber Thieves Exploit Banks' Faith in SWIFT Transfer Network*, Reuters, May 20, 2016, https://www.reuters.com/article/cyber-heist-swift/special-report-cyber-thieves-exploit-banks-faith-in-swift-transfer-network-idUSL2N18H04S.

42 *Banco del Austro, S.A.*, 215 F. Supp. 3d at 305-06.

43 *Id*. at 303.

44 *Id*. at 306.

45 Jonathan Spicer & Ruma Paul, *Bangladesh Eyes Settlement in U.S. Cyber Heist Suit Ahead of Its Own Case*, Reuters, Apr. 16, 2018, https://www.reuters.com/article/us-cyber-heist-bangladesh/bangladesh-eyes-settlement-in-u-s-cyber-heist-suit-ahead-of-its-own-case-idUSKBN1HN1MZ.

46 Baxter Letter, *supra* note 17.

47 Krishna N. Das & Serajul Quadir, *NY Fed, Bangladesh Central Bank to Resume Normal Money Transfers: Sources*, Reuters, Aug. 18, 2016, https://www.reuters.com/article/us-cyber-heist-bangladesh/ny-fed-bangladesh-central-bank-to-resume-normal-money-transfers-sources-idUSKCN10T0VS.

48 *Id*.

49 *Id*.

50 *Cf*. Serajul Quadir & Jonathan Spicer, *In a Shift, Bangladesh Bank Says No Plans to Sue Fed, SWIFT*, Reuters, Aug. 16, 2016, https://www.reuters.com/article/us-cyber-heist-bangladesh/in-a-shift-bangladesh-bank-says-no-plans-to-sue-fed-swift-idUSKCN10R0OG (reporting that Bangladesh Bank officials did not plan to sue the New York Fed).

51 U.C.C. § 4A-202(b) (Am. Law Inst. & Unif. Law Comm'n 2012).

52 U.C.C. § 1-201(b)(2) (Am. Law Inst. & Unif. Law Comm'n 2001).

53 Allision, *supra* note 11 (quoting the New York Fed as stating that "[t]he payment instructions in question were fully authenticated by the Swift messaging system in accordance with standard authentication protocols").

54 Banco del Austro, S.A. v. Wells Fargo Bank, N.A., 215 F. Supp. 3d 302, 305 (S.D.N.Y. 2016)("The court must assess whether the agreed-upon security procedure was commercially reasonable *and* whether the authorizing bank's use of that procedure to authenticate the transfers at issue comported with reasonable commercial standards of fair dealing.).

55 Choice Escrow & Land Title LLC v. Bancorp South Bank, 754 F.3d 611, 623 (8th Cir. 2014).

56 *Id*. The court explained:

> Where . . . a bank's security procedures do not depend on the judgment or discretion of its employees, the scope of the good-faith inquiry under Article 4A is correspondingly narrow. The automation of agreed-upon procedures generally ensures that those procedures will operate in a way that is consistent with the customer's expectations, as long as the procedures do not "unreasonably vary from general banking usage"—in other words, as long as they are commercially reasonable.

Id.

57 *Banco del Austro, S.A.*, 215 F. Supp. 3d at 305.

58 *Cf*. Quadir & Spicer, *supra* note 49 (reporting that Bangladesh Bank would not sue the New York Fed but not providing any reasons for that decision).

59 Ruma Paul, *Bangladesh to Sue Manila Bank Over $81 Million Heist*, Reuters, Feb. 7, 2018, https://www.reuters.com/article/us-cyber-heist-bangladesh/bangladesh-to-sue-manila-bank-over-81-million-heist-idUSKBN1FR1QV.

60 *Bangladesh Open to Out-of-Court Settlement Over $81 Million Cyber Heist*, Reuters, May 3, 2018, https://www.reuters.com/article/us-cyber-heist-bangladesh/bangladesh-open-to-out-of-court-settlement-over-81-million-cyber-heist-idUSKBN1I4218.

61 *See, e.g.*, Spicer & Paul, *supra* note 45 ("There is no act attributable to RCBC which caused the loss or the theft from Bangladesh Bank. . . . We reiterate that RCBC was merely a beneficiary bank, meaning, the payment instructions which are alleged to have been the result of hacking were not executed by it.").

62 *See Bangladesh Open to Out-of-Court Settlement Over $81 Million Cyber Heist, supra* note 60 (reporting that a senior official at Bangladesh Bank said "[t]here is an option before us to settle the issue out of court"); Spicer & Paul, *supra* note 45 (quoting an attorney who noted that given the uncertainty in the applicable law there are an "awful lot of reasons for people to settle").

63 Krishna N. Das et al., *Bangladesh Officials Visit Manila to Seek Recovery of Bank Heist Money*, Reuters, Aug. 1, 2016, https://www.reuters.com/article/us-cyber-heist-bangladesh-philippines-ex/exclusive-bangladesh-officials-visit-manila-to-seek-recovery-of-bank-heist-money-idUSKCN10D0B5 ("Bangladesh Bank is relying on internal RCBC documents to buttress its assertion that the Filipino bank's Jupiter Street branch in Manila . . . delayed acting on requests from RCBC's head office to freeze the funds on Feb. 9, said one of the sources in Dhaka.").

64 U.C.C. § 4A-211(b) (Am. Law Inst. & Unif. Law Comm'n 2012).

65 *Id*. § 4A-211(c). Cancellation of an accepted payment order is also allowed if "a funds-transfer system rule allows cancellation . . . without agreement of the bank." *Id*. There does not appear to be a funds-transfer system cancellation rule applicable to the Bangladesh Bank payment orders.

66 *Id*. §§ 4A-209(b)(1), 4A-205(a). Acceptance also occurs when the beneficiary bank receives payment for the order from the sender or on the funds transfer day following the payment date if the beneficiary bank has access to money from the sender to cover the payment order. *See id*. § 4A-209(2)-(3).

67 *Bangladesh Bank Fund Heist: Stop Payment Orders from Bangladesh Bank "Vague": RCBC*, The Daily Star (Dhaka, Bangladesh), Apr. 12, 2016, https://www.thedailystar.net/business/stop-payment-orders-bangladesh-vague-rcbc-1208086.

68 U.C.C. § 4A-211(c)(2).