Interbank Liability for Fraudulent Transfers *via* SWIFT: *Banco del Austro, S.A. v. Wells Fargo Bank, N.A.*

By Salvatore Scanio

In recent years, criminals have launched cyberattacks on the international banking system through the worldwide bank messaging system known as SWIFT—the Society for Worldwide Interbank Financial Telecommunication. The most highly publicized heist involved $81 million in fraudulent transfers from the Bangladesh Central Bank in February 2016. Hackers "introduced malicious code, known as malware into the Bangladesh bank's server…including keylogger software that monitors strokes on a keyboard, to steal [the bank's] credentials for the Swift system, a closed network used by financial institutions to authorize financial transactions through secure messages."[1] The thieves requested the transfer of $951 million *via* 35 fraudulent SWIFT payment requests from the Bangladesh bank's account at the Federal Reserve Bank of New York to accounts in Sri Lanka and the Philippines.[2] The New York Fed processed five of the 35 orders sending $81 million to the Philippines before the fraud was discovered.[3] The theft was also concealed by malware that "disabled a printer in the Bangladesh bank to prevent officials from reviewing a log of the fraudulent transfers."[4]

There have been reports of several other cases of fraudulent transfers involving SWIFT.[5] According to SWIFT, "a meaningful number of cases" involved attacks similar to the Bangladesh theft.[6] The incidence of SWIFT attacks caused US banking regulators to issue a Joint Statement "to remind financial institutions of the need to actively manage risks associated with interbank messaging and wholesale payment networks."[7] Likewise, SWIFT revised its security procedures, requiring, among other things, member banks to demonstrate annual compliance with the new requirements.[8]

One recent case involving fraudulent transfers *via* SWIFT illustrates the framework for allocating liability between banks in such cases.[9] Banco del Austro, S.A., an Ecuadorian bank, maintained a correspondent banking relationship with Wells Fargo Bank, N.A. in New York in order to conduct international funds transfers. In January 2015 Banco del Austro's computer system was infiltrated by cybercriminals who were able to steal the login credentials of a bank employee, and then logon to the bank's SWIFT terminal and cause at least 13 unauthorized transfers *via* SWIFT by re-issuing previously cancelled or rejected transactions that remained in the bank's SWIFT outbox by altering the amounts, beneficiary, beneficiary bank, and destination. Between January 12, 2015 and January 21, 2015, a dozen SWIFT messages were sent from Banco del Austro to Wells Fargo with fraudulent transfers totaling $12,172,762. Banco del Austro alleged that these transfers were unusual, suspect, or anomalous because they were inconsistent with the bank's normal activity in its correspondent account at Wells Fargo. Specifically, Banco del Austro alleged that the fraudulent transfers were suspicious because:[10]

(1) They were all outside normal operating hours of the bank's SWIFT payment orders;
(2) Many were in unusual amounts, with seven over $1 million;

Salvatore Scanio is a member of the Washington, D.C. law firm, Ludwig & Robinson PLLC, where his practice focuses on domestic and international litigation involving banking, insurance, and other commercial disputes. He attended Tulane University where he earned B.A., M.B.A., and J.D. degrees. Mr. Scanio has more than 20 years of experience in financial litigation, and he advises clients as to liability, defenses, and loss recovery on a wide range of bank and corporate fraud and cybercrime, including check fraud, credit and debit card fraud, wire transfer and ACH fraud, Ponzi schemes, malware attacks, and data breaches. His prior experience includes serving as in-house counsel with a large commercial bank. He is a member of the Federal Reserve System's Secure Payment Task Force, advising the Fed on payment security matters. He may be reached at *sscanio@ludwigrobinson.com* or 202-289-7605.

(3) They had unusual beneficiaries in unusual geographic locations, with nine transfers to Hong Kong;
(4) The frequency of transfer was unusual, with 12 in nine days, with three transfers to the same entity within the span of 26 hours; and
(5) The same entity in Hong Kong received substantial funds from different customers of Banco del Austro within the 26-hour period.

The relationship between Banco del Austro and Wells Fargo was governed by a correspondent banking agreement, set forth in Wells Fargo's "Terms & Conditions for Global Financial Institutions."[11] In January 2016, Banco del Austro brought suit against Wells Fargo for the $12 million in fraudulent funds transfers in New York state court under the New York choice-of-forum clause provided in the agreement.[12] Interestingly, Wells Fargo did not exercise its right to have the dispute submitted to arbitration under the agreement, but instead removed the action to federal court and filed a motion to dismiss for failure to state a claim under Rule 12(b)(6) of the Federal Rules of Civil Procedure.[13]

Banco del Austro asserted causes of action for violations of Uniform Commercial Code (UCC) Article 4A and common law claims of negligence and breach of contract.[14] The correspondent banking agreement's choice-of-law clause provided that it "will be governed by and construed in accordance with Laws of the US and the State of New York, including (without limitation) Articles 4, 4A and 5 of the Uniform Commercial Code . . . ."[15]

Article 4A is the UCC's legal framework governing funds transfers. Generally, UCC Section 4A-204 imposes liability on a receiving bank[16] for unauthorized transfers by requiring the bank to refund any funds (plus interest) from a payment order[17] that was neither: (1) authorized by the customer under UCC Section 4A-202, nor (2) enforceable against the customer under UCC Section 4A-203, as not caused by (a) an authorized employee or (b) a person who obtained access to its transmitting facilities, or otherwise obtained transmittal information from the customer. Thus, whether the risk of loss for an unauthorized transfer falls upon the bank or the customer is governed by UCC Section 4A-202 and 4A-203.[18] Under Subsection 4A-202(a), a payment order is authorized if the person identified as the sender authorized the order or is otherwise bound under the law of agency.[19] Subsection 4A-202(b) further permits the receiving bank to escape liability, even though the customer did not authorize the payment order, if the bank proves:[20]

(1) The bank and customer agreed the authenticity of a payment order would be verified through a "security procedure";
(2) The security procedure agreed upon by the bank and customer is "commercially reasonable";
(3) The bank processed the payment order in "compliance" with the security procedure;
(4) The bank processed the order in compliance with any written agreement or instruction of the customer; and
(5) The bank accepted the payment order in "good faith."

If these five elements are not met, however, the bank will be strictly liable for any unauthorized funds transfer.[21]

In moving to dismiss, Wells Fargo argued that it and Banco del Austro agreed that (1) the funds transfers would be verified by SWIFT authentication procedures and (2) such security procedure was a commercially reasonable method.[22] Under UCC Article 4A, a "security procedure" is a "procedure established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order . . . is that of the customer, or (ii) detecting error in the transmission or the content of the payment order or communication."[23] A "security procedure," however, does not include "procedures that the receiving bank may follow unilaterally in processing payment orders,"[24] such as its internal policies and procedures. The security procedure established in the Wells Fargo correspondent banking agreement provided:[25]

> All payment orders or amendments and cancellations thereof must be transmitted to Wells Fargo in compliance with Security Procedures . . . . The following Security Procedures will be used to verify that Correspondent is the originator of a payment order, or is the sender of other communication requesting an amendment, cancellation or other action regarding a payment order for the communications systems listed below.

> For SWIFT, the SWIFT Authentication procedures in accordance with the SWIFT User Handbook as amended from time to time.... Correspondent agrees that the above described Security Procedures are commercially reasonable in light of Correspondent's circumstances and the type, value and frequency of the payment orders Correspondent will request.

Banco del Austro did "not allege that Wells Fargo failed to adhere to SWIFT authentication procedures,"[26] but maintained that the agreed-upon security procedure included required fraud detection policies and procedures. Banco del Austro pointed to the provision in the agreement that "Wells Fargo is a bank organized and existing under the Laws of the US, and intends to comply with all Laws of the US applicable to it in any of its locations, including without limitation the USA PATRIOT Act,...[and] regulations of the United States Department of the Treasury."[27] Banco del Austro cited the Treasury Department's regulations under the Bank Secrecy Act for correspondent accounts as requiring policies and procedures to detect money laundering activity.[28] Banco del Austro also highlighted a July 31, 2014 letter issued by Wells Fargo about its Global Financial Crimes Management Program that "included identifying unusual activity; automated transaction monitoring; customer surveillance; investigating the unusual activities identified, and determining whether they are suspicious; monitoring customer activity, and apply predictive analysis for customer-centric, cross-channel fraud detection; screening, blocking, and rejecting transactions appropriately; and reporting these matters..."[29]

The court rejected Banco del Austro's argument, finding that the agreement[30]

> "[R]equires only that Wells Fargo adhere to the SWIFT authentication procedures when processing orders received *via* SWIFT. The provision on which Banco del Austro relies did not transform any and all violations of federal and state law into breaches of contract and did not modify the security procedure explicitly outlined under separate header. Thus, Banco del Austro has failed sufficiently to allege that Wells Fargo did not accept the request for the Transfers in compliance with the agreed-upon security procedure."

The court then turned to whether the security procedure was commercially reasonable and whether Wells Fargo acted in good faith. While these are separate inquiries, the court ultimately collapsed its analysis of these two elements.

Under UCC 4A, the issue of "commercial reasonableness of a security procedure is a question of law."[31] Whether the bank complied with the security procedures, however, remains a question of fact.[32] Whether a security procedure is commercially reasonable is determined by considering primarily four factors:[33]

(1) The wishes of the customer expressed to the bank;
(2) The circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank;
(3) Alternative security procedures offered to the customer; and
(4) Security procedures in general use by customers and receiving banks similarly situated.

Under Article 4A, the receiving bank must prove that it processed the payment order in "good faith,"[34] defined as "honesty in fact and the observance of reasonable commercial standards of fair dealing."[35] "Honesty in fact" is measured by a subjective standard, requiring a court to examine the facts surrounding the transaction.[36] The bank's "observance of reasonable commercial standards of fair dealing," however, is evaluated by an objective measurement of the fairness of the party's action in light of prevailing commercial standards.[37] "Although 'fair dealing' is a broad term that must be defined in context, it is clear that it is concerned with the fairness of conduct rather than the care with which an act is performed."[38]

Unsurprisingly, the court in *Banco del Austro* recognized that factual matters outside of the complaint were required to determine whether SWIFT's procedures by themselves constituted a commercially reasonable security procedure and whether Wells Fargo acted in good faith:[39]

> The Court cannot now determine the commercial reasonableness of the agreed-upon security procedure or, by extension, whether Wells Fargo complied with reasonable commercial standards of fair

> dealing when it processed the Transfers pursuant to that procedure. In defining that procedure, the Agreement incorporates wholesale the SWIFT user manual, a document outside of the complaint. Further, both parties in their memoranda urge upon the Court news articles and industry publications detailing the security bonafides and vulnerabilities of the SWIFT system. Resort to these extra-complaint sources illustrates the fact-intensive nature of the commercial reasonableness inquiry, one that courts typically address at summary judgment. At bottom, the facts alleged in the complaint and its exhibits do not permit the Court to rule as a matter of law that use of the SWIFT system, with nothing more, constituted a commercially reasonable security procedure in the context of this particular customer-bank relationship.

Consequently, the court denied Well Fargo's motion to dismiss the claims under UCC Article 4A.[40]

The court, however, granted the motion to dismiss Banco del Austro's contract and negligence claims. The court dismissed the contract claim because Banco del Austro did not allege that Wells Fargo deviated from complying with the "agreed-upon security procedure … [providing for] authentication of orders *via* the SWIFT system in accordance with its user handbook."[41] The court also dismissed the common law negligence claim as displaced by UCC Article 4A.[42]

After the parties conducted discovery, Wells Fargo moved for summary judgment, filing under seal.[43] Before Banco del Austro filed its opposition, the court denied the motion without prejudice.[44] Illustrating the fact-intensive nature of resolving the dispute, the court reasoned that Wells Fargo could raise the same arguments at a bench trial, the parties having waived trial by jury.[45]

Notes

[1] Syed Zain Al-Mahmood, "Hackers Lurked in Bangladesh Central Bank's Servers for Weeks," *The Wall Street Journal*, Mar. 22, 2016, available at *http://blogs.wsj.com/indiarealtime/2016/03/22/hackers-lurked-in-bangladesh-central-banks-servers-for-weeks/* (last accessed on Nov. 21, 2017).

[2] Michael Corkery, "An $81 Million Sneak Attack on the World Banking System," *The New York Times*, May 1, 2016, at 4.

[3] *Id.*

[4] *Id.*

[5] Tom Bergin and Nathan Layne, *Special Report: Cyber thieves exploit banks' faith in SWIFT transfer network,* Reuters (May 20, 2016 3:17 p.m.), available at *http://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD* (last accessed on Nov. 21, 2017).

[6] Tom Bergin and Jim Finkle, *Exclusive: SWIFT confirms new cyber thefts, hacking tactics*, Reuters (Dec. 12, 2016 7:12 p.m.), available at *http://www.reuters.com/article/us-usa-cyber-swift-exclusive-idUSKBN1412NT* (last accessed on Nov. 21, 2017); Jim Finkle, *Second hacker group targets SWIFT users, Symantec warns*, Reuters (Oct. 11, 2016 4:37 p.m.), available at *http://www.reuters.com/article/us-cyber-heist-malware-idUSKCN12B1L3* (last accessed on Nov. 21, 2017).

[7] Federal Financial Institutions Examination Council, *Joint Statement—Cybersecurity of Interbank Messaging and Wholesale Payment Networks* (Jun. 7, 2016), available at *https://www.ffiec.gov/press/PDF/Cybersecurity_of_IMWPN.pdf* (last accessed on Nov. 21, 2017).

[8] Press Release, *SWIFT Introduces Mandatory Customer Security Requirements and An Associated Assurance Framework*, SWIFT (Sept. 27, 2016), available at *https://www.swift.com/insights/press-releases/swift-introduces-mandatory-customer-security-requirements-and-an-associated-assurance-framework* (last accessed on Nov. 21, 2017).

[9] Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. filed Jan. 20, 2016).

[10] Complaint, Doc. No. 1-1, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Jan. 28, 2016), at 5–9.

[11] *Id.* at 2–3.

[12] *Id.*

[13] Def. Wells Fargo Bank, N.A.'s Notice of Removal, Doc. No. 1, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Jan. 28, 2016); Def. Wells Fargo Bank, N.A.'s Mot. to Dismiss, Doc. No. 13, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Feb. 18, 2016).

[14] Complaint, Doc. No. 1-1, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Jan. 28, 2016), at 11-17.

[15] Wells Fargo Bank, N.A., *Terms & Conditions for Global Financial Institutions*, at 14.

[16] A "receiving bank" is the bank receiving the payment order, typically, the customer's bank. UCC § 4A-103(a)(4).

[17] A "payment order" is the instruction to the receiving bank to pay a fixed or determinable amount of money. UCC § 4A-103(a)(1).

[18] UCC § 4A-204(a).

[19] UCC § 4A-202(a).

[20] UCC § 4A-202(b).

[21] UCC § 4A-204(a). Additionally, even if these conditions are met, the risk of loss will still shift to the bank if "the person

committing the fraud did not obtain the confidential information [facilitating breach of the security procedure] from an agent or former agent of the customer or from a source controlled by the customer." UCC § 4A-203 cmt. 5.

22. Def. Wells Fargo Bank, N.A.'s Mem. in Supp. of Mot. to Dismiss, Doc. No. 15, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Feb. 18, 2016), at 9.
23. UCC § 4A-201.
24. UCC § 4A-201 cmt.
25. Wells Fargo Bank, N.A., *Terms & Conditions for Global Financial Institutions*, at 4.
26. Banco del Austro, S.A. v. Wells Fargo Bank, N.A., 215 F. Supp. 3d 302, 304 (S.D.N.Y. 2016).
27. *Id.* at 304; Wells Fargo Bank, N.A., *Terms & Conditions for Global Financial Institutions*, at 14.
28. Plaintiff Banco del Austro, S.A.'s Mem. of Law in Opp. to Def. Wells Fargo Bank, N.A.'s Mot. to Dismiss, Doc. No. 21, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Mar. 31, 2016), at 19-20.
29. *Id.* at 20.
30. *Banco del Austro, S.A.*, 215 F. Supp. 3d at 304.
31. UCC § 4A-202(c). As explained in Article 4A's Official Comments: "It is appropriate to make the finding concerning commercial reasonability a matter of law because security procedures are likely to be standardized in the banking industry and a question of law standard leads to more predictability concerning the level of security that a bank must offer to its customers." UCC § 4A-203 cmt. 4.
32. *Id.*
33. UCC § 4A-202(c).
34. UCC § 4A-202(b).
35. UCC § 4A-105(d)(incorporating definitions in Article 1); UCC § 1-201(20).
36. UCC § 1-201 cmt. 20.
37. UCC § 1-201 cmt. 20.
38. UCC § 1-201 cmt. 20.
39. *Banco del Austro,* 215 F. Supp. 3d at 306 (citations omitted).
40. *Id.*
41. *Id.*
42. *Id.* at 306-307.
43. Def. Wells Fargo Bank, N.A.'s Mem. of Law in Supp. of Mot. for Summary Judgment, Doc. No. 48, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Oct. 3, 2017).
44. Order, Doc. 54, Banco del Austro, S.A. v. Wells Fargo Bank, N.A., No. 1:16-CV-00628 (S.D.N.Y. Oct. 18, 2017).
45. *Id.*