UNC SCHOOL OF LAW

NORTH CAROLINA BANKING INSTITUTE

Volume 11 | Issue 1 Article 16

2007

Secrets Hurt: How SWIFT Shook up Congress, the European Union, and the U.S. Banking Industry

Jeremy S. Shrader

Secrets Hurt: How SWIFT Shook Up Congress, the European Union, and the U.S. Banking Industry

I. INTRODUCTION

Following the devastating events of September 11th, the Bush Administration began an all-out attack on terrorism[1] commonly known as the "War on Terror."[2] Included in this assault was the creation of the Terrorist Finance Tracking Program (TFTP) in 2001, a program designed to prevent future terrorist attacks by identifying and monitoring the financial activity of suspected terrorists both domestically and internationally.[3] A key component to the TFTP was a secret agreement between the U.S. government and a Swiss messaging cooperative known as the Society for Worldwide Interbank Financial Telecommunication (SWIFT).[4] SWIFT is an organization that on a daily basis transmits over its worldwide network millions of messages containing detailed instructions for financial institutions on how to transfer money and other securities.[5] As part of this secret agreement, the United States, through its Office of Foreign Assets Control of the Treasury Department,[6] presented SWIFT with

---

1. *See, e.g.*, Press Release, U.S. Dep't Treasury, Statement of Treasury Secretary John W. Snow on Disclosure of the Terrorist Finance Tracking Program (June 22, 2006), *available at* http://www.treas.gov/press/releases/js4332.htm.

2. Press Release, George W. Bush, President, U.S., Address to a Joint Session of Congress and the American People (Sept. 20, 2001), *available at*: http://www.whitehouse.gov/news/releases/2001/09/20010920-8.html.

3. *See* Press Release, U.S. Dep't Treasury, Terrorist Finance Tracking Program Fact Sheet (June 23, 2006), *available at* http://www.ustreas.gov/press/releases/js4340.htm.

4. *The Terror Financing Tracking Program: Hearing Before the Subcomm. on Oversight and Investigations of the H. Comm. on Financial Servs.*, 109th Cong. (2006) [hereinafter *Hearing*] (statement of Stuart Levey, Under Secretary Terrorism and Financial Intelligence U.S. Department of the Treasury), *available at* 2006 WLNR 11934277.

5. Eric Lichtblau & James Risen, *Bank Data Is Sifted by U.S. to Block Terror*, N.Y. TIMES, June 23, 2006, at A1.

6. SWIFT, EU Parliament Hearing: Swift Statement and Press Release (2006), *available at* http://www.swift.com/index.cfm?item_id=60670.

compulsory subpoenas based on suspected links to terrorism[7] and in exchange received access to specific financial records that contained information highlighting the identities of the sender and recipient, the bank account numbers of each party, and the amount of the transaction.[8] This relationship, known as the SWIFT program, was not only seen as a vital component in the War on Terror,[9] but also as an alternative method of obtaining important financial information that bypassed traditionally burdensome requirements, such as obtaining a search warrant from a judge[10] or following the notification requirements of the Right to Financial Privacy Act (RFPA).[11]

This secret program between SWIFT and the U.S. government was fully exposed this past June when leading U.S. newspapers published detailed reports about the relationship between the two.[12] The subsequent disclosure has ignited a series of problems across the globe that can be broken down into four individually distinct, but, when viewed as a whole, interrelated categories.[13] First, the exposure of the SWIFT program highlights ongoing communication issues between the United States and Europe, specifically the contrasting mindsets on how to mount a war on terrorism without sacrificing individual privacy rights.[14] Second, due to the controversy surrounding the TFTP, SWIFT finds itself caught in the middle of an ongoing predicament between honoring compulsory U.S. subpoenas and complying with European privacy laws.[15] Third, following the publicity of its

7. *See Hearing*, *supra* note 4.

8. *See* Glenn R. Simpson, *Treasury Tracks Financial Data in Secret Program*, WALL ST. J., June 23, 2006, at A1.

9. *See* Press Release, U.S. Dep't Treasury, *supra* note 1.

10. *See* Lichtblau & Risen, *supra* note 5.

11. 12 U.S.C.A. §§ 3401-3422 (West 2000 & Supp. 2006); *see* JENNIFER K. ELSEA & MAUREEN MURPHY, CONG. RESEARCH SERV., TREASURY'S TERRORIST FINANCE PROGRAM'S ACCESS TO INFORMATION HELD BY THE SOCIETY FOR WORLDWIDE INTERBANK FINANCIAL TELECOMMUNICATION (SWIFT) 3 (2006), *available at* http://www.fas.org/sgp/crs/natsec/RS22469.pdf.

12. *See, e.g.*, Josh Meyer & Greg Miller, *Secret U.S. Program Tracks Global Bank Transfers*, L.A. TIMES, June 23, 2006, at A1.

13. *See infra* notes 28-178 and accompanying text.

14. *See* John Ward Anderson, *Belgium Rules Sifting of Bank Data Illegal*, WASH. POST, Sept. 29, 2006, at A14.

15. *Id.*

agreement with SWIFT, the United States not only finds itself embroiled in controversy with the European Union, but also defending its policies domestically as it debates with members of Congress over the legality of the TFTP.[16] More importantly however, the exposure of the SWIFT program forces the United States to evaluate whether its current methods of fighting terrorist financing are effective.[17] Fourth, the revelation of the SWIFT program and its ability to gather important financial information showcases the present tension between the banking industry and the U.S. government over current reporting requirements.[18] Specifically, the existence of the SWIFT program provides the banking industry with support for its assertion that the Financial Crimes Enforcement Network's (FinCEN) proposal mandating that all international transactions be reported by banks[19] is unnecessary and burdensome.[20] This is because the SWIFT program achieves the same end result that the FinCEN program is designed to achieve[21]— the identification of a suspected terrorist's financial activity.[22]

Part II of this Note describes the basic framework and functions of SWIFT, explains the creation, purpose, and authority of the TFTP and highlights the relationship between the two.[23] Part III examines the current controversy surrounding EU concerns over potential privacy law violations committed by SWIFT in its arrangement with the United States as well as discussing the difficult situation in which SWIFT has found itself—

16. R. Christian Bruce, *Rep. Kelly Asks GAO to Review Terrorist Finance Tracking Program*, 87 BANKING REP. 94, 94 (2006).

17. *See* John Sandman, *Terrorist Tracking, Five Years On: Controversy Over SWIFT May Have Been Misplaced,* SEC. INDUSTRY NEWS, Sept. 25, 2006; Simpson, *supra* note 8.

18. *See* Rob Blackwell, *A Sharp Split on 'Report All Wires' Idea*, AM. BANKER, Apr. 12, 2005, at 1.

19. Press Release, Fin. Crimes Enforcement Network, FinCEN Seeks Industry Input on Feasibility of Collection of Cross-Border Wire Transfer Data (Mar. 10, 2006), *available at* http://www.fincen.gov/fincennewsrelease03102006.html; *see* Press Release, U.S. Dep't Treasury, *supra* note 3.

20. *See* Joe Adler, *Fed to FinCEN: Weigh Cost of Transfer Report Idea; Reporting of International Wire Transfers Proposed by Financial Crimes Enforcement Network*, AM. BANKER, July 11, 2006, at 3.

21. *Id.*

22. *Id.*

23. *See infra* notes 28-63 and accompanying text.

stuck between the competing security interests of the United States and the privacy interests of the European Union.[24] Part IV focuses on domestic concerns regarding SWIFT and the TFTP in Congress[25] and analyzes whether some of the current methods of the TFTP are effective in the ongoing War on Terror.[26] Lastly, Part V discusses the present tension between the U.S. government and the banking industry and how the SWIFT program may make bankers' lives easier in light of the ongoing FinCEN proposal requiring banks to report all international wire transactions.[27]

II. BACKGROUND

A. *The Society for Worldwide Interbank Financial Telecommunications (SWIFT)*

In its most basic sense, SWIFT is a messaging system "overseen by a committee drawn from major central banks"[28] and used by banks participating in international wire transfers.[29] SWIFT is owned by "banks, broker-dealers, and investment managers," and consists of close to 8,000 worldwide financial institutions.[30] However, SWIFT is not considered a bank and does not have individual customers; instead it acts as "an intermediary for financial institutions."[31] In this role, rather than performing the actual transaction, SWIFT provides instructions in the form of messages on how to transfer money between financial institutions across the globe.[32] In a normal day, the SWIFT network handles close to 12 million messages, and in 2005 transmitted 2.5 billion

24. *See infra* notes 64-100 and accompanying text.

25. *See infra* notes 101-27 and accompanying text.

26. *See infra* notes 101-27 and accompanying text.

27. *See infra* notes 128-79 and accompanying text.

28. Press Release, U.S. Dep't Treasury, *supra* note 3. SWIFT's committee consists of "the U.S. Federal Reserve, the Bank of England, the European Central Bank, the Bank of Japan, and the principal director, the national Bank of Belgium." *Id.*

29. *See Hearing*, *supra* note 4.

30. *See* Press Release, SWIFT, *supra* note 6.

31. Press Release, U.S. Dep't Treasury, Legal Authorities Underlying the Terrorist Finance Tracking Program (June 23, 2006), *available at* http://www.ustreas.gov/press/releases/js4340.htm.

32. *See* Lichtblau & Risen, *supra* note 5.

financial messages.[33] In providing directions on how to carry out these transactions, SWIFT has created and currently maintains large databases of confidential information[34] that include the identities of the sender and recipient of the transaction, the bank account numbers of the parties, and the amount of the transaction.[35] Since SWIFT databases—some of which are located in the United States—contain secret financial information, the organization places a premium on securing the confidentiality of its users' information[36] and prides itself on its reputation as one the safest networks in the world.[37]

B. The Terrorist Finance Tracking Program (TFTP)

Following September 11th, President Bush declared a national emergency in order to deal with the effects of the terrorist attacks while at the same time taking the necessary steps to prevent future strikes.[38] In implementing these preventive measures, the President issued Executive Order 13224[39] which granted the U.S. Treasury Department the discretion and authority "to use all appropriate measures to identify, track, and pursue not only those persons who commit terrorist acts here and abroad, but also those who provide financial or other support for terrorist activity."[40] In exercising its newfound powers, the Treasury Department created the TFTP in order to identify, monitor, and follow suspected terrorists, as well as individuals and organizations that finance suspected terrorists.[41]

The ability of the President to issue an executive order and then delegate that authority to the Treasury Department

33. *See* Meyer & Miller, *supra* note 12.

34. *Id.*

35. *See* Simpson, *supra* note 8.

36. *See* Press Release, Soc'y for Worldwide Interbank Fin. Telecomm., Update and Q&A to SWIFT's 23 June 2006 Statement on Compliance (Apr. 25, 2006), *available at* http://www.swift.com/index.cfm?item_id=60275.

37. *See* Meyer & Miller, *supra* note 12. A former SWIFT executive said that SWIFT "is arguably the most secure network on the planet," and even compared the security of SWIFT's databases to Fort Knox. *Id.*

38. *See* Press Release, U.S. Dep't Treasury, *supra* note 31.

39. Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 23, 2001).

40. Press Release, U.S. Dep't Treasury, *supra* note 3.

41. *Id.*

originated in part under the International Emergency Economic Powers Act (IEEPA)[42] and the United Nations Participation Act (UNPA).[43] The IEEPA allows the President—after declaring a state of emergency based on the presence of an extraordinary threat to the security of the United States—to employ a wide-range of powers.[44] Included in this authority is the ability to access financial transactions or transfers occurring between banking institutions that "involve any interest of any foreign country or a national thereof."[45] Likewise, the UNPA authorizes the President to "implement measures ordered by the United Nations Security Council,"[46] such as monitoring financial relationships and transactions between foreigners and the United States.[47] Consequently, the Treasury Department quickly created the TFTP in order to identify and monitor the financial transactions of suspected terrorists and those individuals or organizations that financed them.[48]

C. *The Relationship Between SWIFT and the TFTP*

Ironically, when the TFTP was created, members of the Bush Administration were unaware of the vast amount of valuable financial data contained in SWIFT's databases.[49] This source of information was not recognized until a Wall Street executive suggested to a key member of the administration that accessing SWIFT's databases could be a valuable tool in the War on Terror.[50] This suggestion hit home with the administration, especially because evidence uncovered after September 11th showed that nine out of the eleven terrorists received money to help fund the deadly plot via international wire transfers from

42. 50 U.S.C.A §§1701-1706 (West 2000 & Supp. 2006).

43. *See* ELSEA & MURPHY, *supra* note 11, at 3-5.

44. *Id.* at 2. The President can "exercise broad powers over property or financial transactions, including transfers of credit or payments through banking institutions and securities or other obligations." *Id.*

45. 50 U.S.C.A § 1702(a)(1)(A)(ii).

46. ELSEA & MURPHY, *supra* note 11, at 5.

47. 22 U.S.C. § 287(c) (2000).

48. *See* Press Release, U.S. Dep't Treasury, *supra* note 3.

49. *See* Lichtblau & Risen, *supra* note 5.

50. *Id.*

Europe and the Middle East to banks in the United States.[51] Consequently, as soon as the administration learned that it could identify and monitor terrorist activity by accessing SWIFT's financial records that included information on international transfers, the Treasury Department began to obtain financial information from SWIFT through the use of compulsory subpoenas.[52]

As noted by Treasury officials, the use of compulsory subpoenas (also known as administrative subpoenas) is a novel concept.[53] Whereas access to individual financial records typically occurs through the issuance of a subpoena that has first been approved for example by a grand jury,[54] compulsory subpoenas bypass this procedural requirement.[55] Instead, Treasury officials create a compulsory subpoena pursuant to their delegated powers from the President that originate under the IEEPA,[56] present the subpoena to SWIFT officials, and obtain access to specific financial records in SWIFT's databases as long as there is a suspected link to terrorism.[57] Additionally, due to its substantial business and operations in the United States, SWIFT is subject to federal jurisdiction and is required to cooperate with these compulsory subpoenas.[58]

Yet, in administering these broad subpoenas, U.S. officials do not have complete freedom to browse through all of SWIFT's financial records.[59] Instead, the subpoenas only grant U.S. officials access to specific financial files that have some relationship to either a terrorist or a terrorist organization.[60] In addition to this limitation placed on government officials, additional safeguards

51. *Id.*

52. *See* Press Release, U.S. Dep't Treasury, *supra* note 31.

53. *See* Simpson, *supra* note 8.

54. *See* Lichtblau & Risen, *supra* note 5.

55. *See* Simpson, *supra* note 8.

56. *See Hearing*, *supra* note 4. IEEPA "allows the government to compel the production of information pursuant to Presidential declarations of national emergency." *Id.*

57. *Id.*

58. *See* Press Release, Soc'y for Worldwide Interbank Fin. Telecomm., *supra* note 36. For example, SWIFT must abide by lawful U.S. subpoenas because one of its financial databases is located in the U.S. *See* Simpson, *supra* note 8.

59. *See* Press Release, U.S. Dep't Treasury, *supra* note 3.

60. *See* Press Release, U.S. Dep't Treasury, *supra* note 31.

were put in place in order to prevent abuse of financial information and allow SWIFT some level of control over the subpoenaed data.[61] These protective mechanisms include the presence of SWIFT representatives who oversee all searches and possess the authority to stop any and all searches that they feel do not have a sufficient link to terrorism.[62] Additionally, each search is recorded and reviewed by both an internal and external auditor to ensure that the searches are limited to financial activities related to terrorism.[63]

III. SWIFT PROGRAM IGNITES CONCERNS IN THE EUROPEAN UNION

A. Controversy in Europe

The public revelation of the TFTP's use of SWIFT's financial databases highlights the ongoing communication flaws between the United States and Europe, specifically the differing views on how to balance the demands of fighting terrorism[64] with the protection of individual privacy rights.[65] EU governments' disapproval of the TFTP's use of SWIFT can be traced to two reasons: (1) high-ranking European governmental officials were unaware of the SWIFT program[66] until American newspapers revealed its existence in June of 2006;[67] and (2) the SWIFT

61. *See* Press Release, Soc'y for Worldwide Interbank Fin. Telecomm., *supra* note 36.

62. *See Hearing*, *supra* note 4.

63. *See* Press Release, Soc'y for Worldwide Interbank Fin. Telecomm., *supra* note 36.

64. *See* Press Release, U.S. Dep't Treasury, *supra* note 3.

65. *See* Lichtblau & Risen, *supra* note 5. Top United States officials do not believe that individuals have a privacy interest in their financial information contained in international wire transactions. *Id.* On the other hand, German officials believe European law places a greater emphasis on privacy laws than does the United States. Niels C. Sorrells, *German Data Security Officials Question SWIFT System Security*, 87 BANKING REP. 795, 795-96 (2006).

66. Bengt Ljung, *Belgian Leader Says SWIFT Broke Law by Providing Bank Transfer Data to U.S.*, 87 BANKING REP. 496, 496-97 (2006).

67. *See* ELSEA & MURPHY, *supra* note 11, at 1.

program, according to EU officials, violates European privacy laws.[68]

A report from the European Parliament echoed what other European countries[69] and governmental bodies had been saying about the SWIFT program—that the relationship involved violations of "various articles of the EU data protection rules, especially ones that require private persons to be made aware that their data is being transferred."[70] Additionally, officials have voiced their displeasure with the SWIFT program by noting that according to European law, confidential personal data may only be transferred to another country if that country provides adequate protections; the principal problem being that European governments do not believe the United States offers sufficient protections to financial records.[71]

Although EU governments and officials are concerned over purported privacy violations, the real source of their frustration appears to be the simple fact that many of them were not aware of the existence of the SWIFT program.[72] In other words, it is possible that they are upset because they were not important enough to be included in the secret agreement.[73] Although this assumption may appear to be childish, it is supported by the fact that SWIFT's attempts to respond to the

68. *See* Joe Kirwin, *Trichet Calls for Wire Transfer Pact Addressing Anti-Terror, Data Protection Needs*, 97 BANKING REP. 544, 544 (2006).

69. *See* Sorrells, *supra* note 65. German Data Security officials concluded in a study of their own that SWIFT violated German and European Union protection laws and highlighted the fact that European law has higher privacy standards than American law does. *Id.*

70. *See* Kirwin, *supra* note 68.

71. *SWIFT hits back at EU criticism*, ELECTRONIC PAYMENTS INT'L, Oct. 24, 2006, at 1.

72. *See* Anderson, *supra* note 14.

73. *Id.* Belgium's Data Privacy Commission released a 20-page report stating that at least European officials should have been notified of the SWIFT program from the very beginning. *Id.* In addition to being upset at SWIFT, the supervisor of European Data Protection was also angered that the European Central Bank (ECB), who had knowledge of the SWIFT program, chose not to inform other leading officials. *See* Ljung, *supra* note 66. The Prime Minister of Belgium also believed that the current problem could have been made easier had SWIFT officials notified European institutions and the Belgian government in order "to anticipate and discuss additional guarantees." *Id.*

Belgian Commission's report on potential violations were not granted until after the report went public.[74]

Interestingly enough, even in light of purported privacy violations and adamant discontent with being excluded from the existence of the SWIFT program, European governments are not taking, nor do they plan to take, any legal action against SWIFT or the United States.[75] Instead, they agree that the program's existence is vital to preventing terrorism, yet have requested that the United States and European Union find a way to bring the program into compliance with European law.[76] In other words, EU governments seek a concrete agreement on how to effectively fight terrorism while at the same time protecting Europeans' individual privacy rights.[77] SWIFT officials have echoed this sentiment.[78]

While some European governments have called for U.S. participation in order to solve the current problem, other European governments have developed possible solutions that do not involve American cooperation.[79] German privacy officials have offered three possible answers to the privacy concerns facing SWIFT suggesting that (1) SWIFT move all of its data servers to European countries and out of the United States so that the financial information stored on the databases would be subject only to European privacy laws; (2) there be a higher level of encryption on the financial information so that U.S. officials cannot view the information; and (3) all banks inform their customers that under the current system their financial information may not be secure.[80] Although all three resolutions seem viable, the officials themselves have acknowledged the

74. *See SWIFT hits back at EU criticism*, *supra* note 71.

75. *See* Anderson, *supra* note 14.

76. *Id.*

77. *Id.*

78. Sarah Litner & Michael Peel, *SWIFT Post-9/11 Privacy Breach*, FIN. TIMES, Nov. 24, 2006, International Economy and Americas at 8. *SWIFT* wants a quick resolution to the controversy between the United States and European Union regarding potential privacy violations and representatives of the messaging organization have been adamant in voicing their desire for the creation and implementation of a mechanism that provides SWIFT with "legal security" when dealing with future requests of financial information by the United States. *Id.*

79. *See* Sorrells, *supra* note 65.

80. *Id.*

unlikelihood of their solutions gaining much support within the German banking industry since implementing any of these rules could potentially ban certain banks from offering international transactions and consequently harm business.[81] Interestingly, it is important to note that in all three instances, German privacy officials focused solely on privacy issues rather than evaluating what effects these potential solutions would have on helping or harming the prevention of future terrorist attacks.[82]

B. SWIFT: Caught in the Middle of the Controversy

Stuck in the middle between the European Union's fight for privacy and the United States' War on Terror, SWIFT faces the difficult proposition of abiding by compulsory U.S. subpoenas[83] while at the same time walking the fine line of not violating European privacy laws.[84] Since SWIFT maintains business, offices, and databases both in Europe and in the United States, the organization is subject to both American[85] and European jurisdiction.[86]

As a result of the controversy over the SWIFT program, SWIFT has experienced problems in its relationship with EU governments.[87] SWIFT took great offense to the barrage of accusations[88] aimed at the messaging service accusing SWIFT of repeatedly violating European privacy laws by granting U.S. officials access to its financial databases.[89] Whether in response to a report from the Belgian national data protection authority,[90] an

81. *Id.*

82. *Id.*

83. *See* Press Release, US Dep't Treasury, *supra* note 31.

84. *See* Kirwin, *supra* note 68.

85. *See* Press Release, Soc'y for Worldwide Interbank Fin. Telecomm., *supra* note 36.

86. *See* Kirwin, *supra* note 68.

87. *See* Ljung, *supra* note 66. Belgian Prime Minister Guy Verhofstadt said that SWIFT violated its obligations relating to protecting personal privacy information under Belgian law. *Id.*

88. *Id.*

89. *See SWIFT hits back at EU criticism, supra* note 71.

90. *See* Kirwin, *supra* note 68.

accusation from EU data protection officials,[91] or a study from German privacy officials[92] (all three of which accused SWIFT of violating European privacy laws), SWIFT has remained adamant in its stance that it complies with applicable European and American laws when providing information to the United States.[93] Additionally, SWIFT notes that it has received repeated assurances from the United States that the information it turns over is only being used in terrorism investigations[94] and that the information is protected in a secure environment.[95] Yet, this explanation is not sufficient in the eyes of some EU governments.[96]

In its most basic sense, the disagreement between EU governments and SWIFT regarding compliance with European privacy laws can be explained by a difference in interpretation of what type of messaging service SWIFT is and, consequently, what European privacy laws are applicable.[97] For example, according to Belgian law, whether or not an organization is subject to certain privacy laws depends on its classification as either a data processor or a data controller.[98] Financial institutions that act as data controllers have a contractual obligation to protect their client's financial information whereas financial institutions labeled as data processors do not.[99] SWIFT claims that since it is not a bank and as a result neither carries out the transaction nor acts as a financial institution, it is considered a data processor and is exempt from specific Belgian privacy laws.[100]

---

91. Joe Kirwin, *EU Data Privacy Officials Probing Possible Data Protection Breaches in SWIFT Matter*, 87 BANKING REP. 238, 238 (2006).

92. *See* Sorrells, *supra* note 65.

93. *See SWIFT hits back at EU criticism*, *supra* note 71.

94. *Id.*

95. *See* Press Release, Soc'y for Worldwide Interbank Fin. Telecomm., *supra* note 36. Subpoenaed data is stored in an extremely secure environment and is treated with the highest security and confidentiality according to SWIFT. *Id.*

96. *See SWIFT hits back at EU criticism*, *supra* note 71.

97. *Id.*

98. *Id.*

99. *Id.*

100. *Id.*

IV. CONCERNS REGARDING SWIFT AND THE TFTP IN THE U.S. CONGRESS

The subsequent exposure of the arrangement between the U.S. government and SWIFT highlights the United States' own internal communication struggles with Congress[101] and also questions the effectiveness and legality of the government's current methods of the TTFP.[102] Up until the June 2006 newspaper reports exposed the existence of the SWIFT program as part of the TFTP,[103] only certain members of Congress knew about the relationship between SWIFT and the Treasury Department.[104] However, in citing the requirements of IEEPA,[105] other members of Congress (like many of their European counterparts),[106] felt that they were not adequately informed about the program's existence and the methods in which the program obtained financial information.[107]

A. Controversy Within Congress over Legality of SWIFT Program

Not only is there debate over whether Congress was properly informed of the SWIFT program, there is also evidence supporting the assertion that members of Congress are currently split on whether the TFTP is legally valid; specifically whether the SWIFT program violates U.S. citizens' privacy rights when the

101. *See* Bruce, *supra* note 16.

102. *See* ELSEA & MURPHY, *supra* note 11, at 2-3.

103. *See* Lichtblau & Risen, *supra* note 5.

104. *See* Press Release, U.S. Dep't Treasury, *supra* note 31. Stuart Levey, Under Secretary Terrorism and Financial Intelligence in the U.S. Department of the Treasury, testified that congress was properly informed of the Terrorist Finance Tracking Program which included the SWIFT program. *Id.*

105. *See* Bruce, *supra* note 16. As the legal foundation for the compulsory subpoenas issued to SWIFT, the International Emergency Economic Powers Act (IEEPA) contained congressional notification requirements that were not sufficiently followed according to House Financial Oversight and Investigations Subcommittee Chair Sue Kelly. *Id.*

106. *See* Ljung, *supra* note 66.

107. *See* Bruce, *supra* note 16. The IEEPA mandates that "the President, in every possible instance, shall consult with Congress before exercising any of the authorities granted by this chapter and shall consult regularly with the Congress so long as such authorities are exercised." 50 U.S.C.A. § 1703 (West 2000 & Supp. 2006).

financial records pertain to Americans.[108] Historically speaking, the Constitution itself does not provide any inherent protection "against governmental access to financial information turned over to third parties."[109] In response to this, Congress passed the Right to Financial Privacy Act of 1978 (RFPA), which granted individuals some protection from the government accessing their financial records.[110] Normally, the RFPA mandates that individuals receive notice from government officials when they seek access to their individual financial information.[111] In addition to providing notice to the individual, officials must present the financial institutions with a device such as an administrative subpoena in order to obtain access to the customer's financial information.[112] However, these requirements only pertain to depository institutions such as banks.[113] Since U.S. officials determined that SWIFT is considered a banking cooperative and not a bank, the protections of individuals' financial privacy rights as documented in the RFPA do not apply when the Treasury Department issues compulsory subpoenas to SWIFT in exchange for access to confidential financial information.[114] Thus, one of the principal advantages of compulsory subpoenas is that officials do not have to present administrative subpoenas to banks nor do they have to give notice to the suspected individual whose financial records they wish to access.[115]

While on its face this legal analysis by government officials appears to be valid, even high ranking Treasury Department officials admit that the use of broad, compulsory subpoenas in an acknowledged financial "grey area"[116] is a method of accessing financial data that has not previously been attempted.[117]

---

108. *See* Bruce, *supra* note 16.

109. *See* ELSEA & MURPHY, *supra* note 11.

110. *See* Lichtblau & Risen, *supra* note 5.

111. *Id.*

112. 12 U.S.C.S. §§ 3405, 3408 (2006); *see Hearing*, *supra* note 4. Also known as a compulsory subpoena, an administrative subpoena is an order that compels an individual or organization to provide certain information. *See* Simpson, *supra* note 8.

113. 12 U.S.C.S. § 3401 (2006).

114. *See* Lichtblau & Risen, *supra* note 5.

115. *See* ELSEA & MURPHY, *supra* note 11 ; Lichtblau & Risen, *supra* note 5.

116. *See* Lichtblau & Risen, *supra* note 5.

117. *See* Simpson, *supra* note 8.

Consequently, members of Congress remain split on the issue.[118] For example, immediately following the June 2006 news revelations, the House of Representatives demonstrated its support of the TFTP by passing House Resolution 895, which specifically supports intelligence and law enforcement programs that track terrorists and their finances such as the TFTP.[119] However, shortly thereafter, other members of Congress who feared potential privacy violations ordered an investigation (the results of which have not yet been released) into the legality of the TFTP.[120]

B. *Is the SWIFT Program an Effective Component of the TFTP?*

One looming question regarding the exposure of the SWIFT program is whether or not the program remains an effective tool in the War on Terror.[121] For the most part, government officials believe the exposure of the TFTP's relationship with SWIFT damaged[122] a successful terrorist financing tracking program with documented results.[123] Yet, these same officials believe that the SWIFT program will continue to be an effective tool in the War on Terror by identifying lower to mid-level terrorists and their financers—individuals who believe they can elude detection by using international wire transactions to

118. *See infra* notes 119-20 and accompanying text.

119. H.R. Res. 895, 109th Cong. (2006).

120. *See* Bruce, *supra* note 16. Chair of the House Financial Oversight and Investigations Subcommittee requested that Comptroller General David M. Walker conduct an investigation about the Terrorist Finance Tracking Program "to ensure that it was indeed conducted in accordance with all proper laws, that it does possess all necessary safeguards, and that Congress was adequately informed." *Id.*

121. *See* Press Release, U.S. Dep't Treasury, *supra* note 31.

122. *See* Simpson, *supra* note 8. In a statement to the *Wall Street Journal*, Stuart Levey admitted that he feared that "sophisticated terrorists will now stop using the system in ways we have access to, or will take extensive precautions to hide their identities, and that is really a loss." *Id.*

123. *See* Press Release, U.S. Dep't Treasury, *supra* note 31. TFTP helped capture the terrorist known as Hambali, the mastermind behind the 2002 Bali bombings. *Id.* SWIFT program also had domestic success when it helped capture and convict a Brooklyn man, Uzair Paracha, for providing funds to an Al Qaeda operative in Pakistan when he agreed to channel $200,000 to a terrorist cell through a Karachi bank in 2005. *See* Lichtblau & Risen, *supra* note 5.

transfer funds.[124] However, others note that the SWIFT program is an example of an outdated messaging system[125] that sophisticated terrorists no longer use.[126] Interestingly, Treasury officials themselves have acknowledged the overall trend of terrorists moving away from typical international wire transfers and instead relying on cash couriers and other informal methods of transferring money.[127]

V. SWIFT PROGRAM HIGHLIGHTS CONCERNS WITHIN BANKING INDUSTRY

A. Current Reporting Requirements for Banks

The banking industry is subject to such reporting requirements as those implemented under the Bank Secrecy Act (BSA)[128] and Title III of the USA PATRIOT Act.[129] Passed in 1970, the BSA mandates that banks maintain records and file reports containing information relating to criminal, tax, and regulatory matters.[130] After these documents are filed with FinCEN,[131] international and domestic law enforcement agencies, the Federal Reserve, and other bank supervisory agencies[132] inspect the reports in order "to identify, detect and deter money laundering whether it is in furtherance of a criminal enterprise,

124. *See* Meyer & Miller, *supra* note 12.

125. Dan Barnes, *Is Swift Living in the Past?*, THE BANKER, Oct. 1, 2006, at 20.

126. *See* Sandman, *supra* note 17.

127. *See Hearing*, *supra* note 4.

128. 12 U.S.C. § 1829(b) (2000).

129. 31 U.S.C.A. § 5318A (West 2000 & Supp. 2006); *see* ELSEA & MURPHY, *supra* note 11, at 4.

130. Internal Revenue Service, U.S. Dep't Treasury, Suspicious Activity Reports, http://www.irs.gov/businesses/small/article/0,,id=154555,00.html (last visited Jan. 25, 2007).

131. *See The Bank Secrecy and the USA PATRIOT Act: H. Before the Comm. on Int'l Relations*, 107th Cong. (2004) (statement of Herbert A. Biern, Senior Associate Director Division of Banking Supervision and Regulation), *available at* http://www.federalreserve.gov/boarddocs/testimony/2004/20041117/default.htm. Even though the Treasury Department has statutory authority to oversee the BSA, it has elected to delegate this regulatory authority to FinCEN, a bureau of the Treasury Department. *Id.* With this power, FinCEN informs banks about regulations, offers assistance on how to comply with the rules, and pursues violators in specific situations. *Id.*

132. *Id.*

terrorism, tax evasion or other unlawful activity."[133] Passed in response to September 11th, the USA PATRIOT Act includes anti-money laundering laws that increase the various customer identification requirements for banks under the BSA while simultaneously criminalizing the financing of terrorism.[134]

In following the BSA and the purpose of the USA PATRIOT Act,[135] banks must file suspicious activity reports (SARs)[136] when they detect a violation of the BSA or observe a suspicious transaction related to money laundering.[137] In relation to terrorism, SARs are seen as an effective tool in the War on Terror[138] since banks must file SARs if they identify suspicious activities related to terrorist financing.[139] The triggers for filing a SAR include when "the funds come from illegal activity or disguise funds from illegal activity; the transaction is structured to evade BSA requirements or appears to serve no known business or apparent lawful purpose; or the money services businesses (MSB) is being used to facilitate criminal activity."[140] The penalty for failing to file a SAR can be severe.[141] For example, in October of 2005, AmSouth Bank was fined $40 million by the U.S. Attorney's Office for the Southern District of Mississippi for failing to file SARs.[142]

Scared over potential prosecution and heavy fines and uncertain about when reporting requirements such as those of a SAR apply, banks have pointed to SARs as an example of the

133. *Id.*

134. *Id.* The PATRIOT Act prohibits banks from participating in business affairs with foreign shell banks, mandates that banks increase their protective mechanisms for accounts involving foreign correspondents and private banking accounts, and calls for a better relationship between banks and the U.S. government regarding the sharing of financial information. *Id.*

135. 50 U.S.C.S. § 1861 (2001).

136. 31 U.S.C.A § 5318A (West 2000 & Supp. 2006).

137. 12 C.F.R. § 21.11 (2000).

138. *See* Internal Revenue Service, *supra* note 130.

139. *Trends and Analysis: Terrorist Financing Suspicious Activity Reports*, SAR Activity Rev. (FinCEN, Washington, D.C.), Apr. 2005, at 5-6, *available at* http://www.fincen.gov/sarreviewissue8.pdf.

140. *See* Internal Revenue Service, *supra* note 130.

141. Rob Blackwell, *FinCEN Figures Show SAR Glut is Worsening*, AM. BANKER, Apr. 15, 2005, at 1.

142. *Id.*

problems with the current reporting requirements.[143] Specifically, banking industry officials believe that law enforcement agencies are ill-suited to properly handle and search for criminal activity in the large amount of information that banks are currently required to provide.[144] In addition, members of the banking industry believe that in some instances law enforcement agencies are not even analyzing the information that they report.[145] FinCEN, which receives the reports from the banks, has responded to these criticisms by claiming that any shortcoming on its part to properly scan financial information for potential criminal activity is a direct result of the banking industry's increase of unnecessary and defensive SARs.[146] Even though banking officials themselves have accepted blame for the huge number of SARs,[147] it appears that until reporting requirements are made clear, banks will continue to file more and more SARs and law enforcement agencies will arguably struggle to properly analyze the data.[148] Consequently, potential terrorists could fall through the cracks.[149]

B. Criticizing the FinCEN Proposal

Although the disclosure of the SWIFT program has provided the banking industry with an opportunity to criticize current banking requirements, it has primarily allowed the banking industry to condemn and denounce FinCEN's proposal mandating that banks report all international wire transactions.[150] The Intelligence Reform and Prevention Act of 2004[151] authorized the

143. *Id.*

144. Rob Blackwell, *Reacting to SWIFT: Hot, Cold, and Both: Some Back Efforts as Others Cite Privacy; Fed Is Subpoenaed; Reaction to Government Monitoring of International Wire Transfers*, AM. BANKER, June 26, 2006, at 1.

145. Stacy Kaper, *2d Thoughts at FinCEN About Extra Wire Data*, AM. BANKER, Apr. 24, 2006, at 5.

146. *See* Blackwell, *supra* note 141.

147. *Id.* Statistics show that banks filed record levels of SARs in March of 2005 with 43,549 reports, a 40% increase over the previous March. *Id.*

148. *See* Blackwell, *supra* note 141; Blackwell, *supra* note 144.

149. *See* Blackwell, *supra* note 141; Blackwell, *supra* note 144; Kaper, *supra* note 145.

150. *See* Kaper, *supra* note 145.

151. Intelligence Reform and Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (codified at 31 U.S.C.A. § 5318(n)(1) (2006)).

Secretary of the Treasury Department to mandate (and which was mandated) that certain financial institutions such as banks report to FinCEN all international wire transactions.[152] The purpose of this requirement was to obtain important information regarding terrorist funding and money laundering.[153] Before this mandate can take effect, however, the IRPA requires that a feasibility study be performed by FinCEN that outlines: (1) situations in which financial information would be relevant to a terrorist investigation; (2) the form, content, and frequency of such reports from banks; (3) the necessary technology required for FinCEN to properly analyze the information and delegate the information to other law enforcement agencies for analysis; and (4) the required information security protections.[154] After completing the study, FinCEN must then give the report to Congress as well as to the Treasury Secretary who is responsible for the final approval.[155] While FinCEN has completed its study and presented it to the Treasury Secretary for approval, FinCEN officials have publicly announced that there is no way that the changes will take place by the end of 2007 and instead any new approved regulations will be implemented over time.[156] Although the specifics of the feasibility study have not been released to the public, the common understanding among FinCEN officials and members of the banking industry is that the proposal broadly requires banks to report all international wire transfers.[157]

As recognized by both banking and FinCEN officials, the government does not want to impose unnecessary reporting burdens on financial institutions.[158] Yet, whether or not the

152. *Id.* § 6302, 118 Stat. at 3748-49 (codified at 31 U.S.C.A. § 5318(n)(1) (2006)).

153. *See FinCEN Seeks Industry Input on Feasibility of Collection of Cross-Border Wire Transfer Data*, BANKING & FIN. SERVICES POL'Y REP., June 2006, at 24.

154. Intelligence Reform and Prevention Act § 6302, 118 Stat. at 3749 (codified at 31 U.S.C.A. § 5318(n)(4)(A) (2006)).

155. R. Christian Bruce, *Money Laundering: Treasury Reviews Proposal to Require Reporting Cross-Border Wire Transfers*, 87 BNA BANKING REP. 553, 553 (2006).

156. *Id.* Initially, if any new reporting regulations were to be implemented, they were to take place before December 2007. Intelligence Reform and Prevention Act § 6302, 118 Stat. at 3750 (codified at 31 U.S.C.A. § 5318(n)(5)(A) (2006)).

157. *See* Adler, *supra* note 20.

158. *FinCEN Seeks Industry Input on Feasibility of Collection of Cross-Border Wire Transfer Data*, *supra* note 153.

proposal presents the banking industry with needless regulations depends on which party you ask.[159] From a banking perspective, there are four primary criticisms of the FinCEN reporting proposal: (1) the report does not take into consideration the potential economic effect on banks in terms of replacing below-par technology systems with new and improved technology systems capable of distinguishing between domestic and international wire transfers;[160] (2) requiring this kind of technology system may prevent financial institutions from remaining competitive in the global market since the FinCEN proposal could potentially prohibit U.S. financial institutions from creating and using cutting-edge payment systems;[161] (3) the FinCEN reporting requirement is unnecessary in light of the fact that the SWIFT program achieves the same end result[162] by identifying and monitoring the financial activity of terrorists;[163] and (4) as evidenced by law enforcement agencies' supposed difficulty in analyzing and handling the vast number of SARs,[164] industry officials are unsure how law enforcement officials could possibly handle the additional workload caused by the new FinCEN reporting proposal.[165]

In recognizing the banking industry's concerns regarding the new proposal such as those relating to compliance costs, the effect on the U.S. electronic transfer system as a whole, and privacy protections,[166] high ranking FinCEN officials have responded vaguely by saying that these concerns will be addressed

159. *See infra* notes 161-75 and accompanying text.

160. *See* Kaper, *supra* note 145. According to experts in the banking industry, the current wire structure of some banks presents a challenge in complying with a proposal requiring banks to report all international wire transactions—namely that the existing wire structure is varied and "much of it doesn't enable institutions to report the difference between cross-border and domestic wire transfers," according to Richard Riese, the director of the American Bankers Association's Center for Regulatory Compliance. *Id.*

161. *See* Adler, *supra* note 20. This was an argument proposed by the Federal Reserve Board, suggesting that this potential effect be taken into consideration while FinCEN performed its study. *Id.*

162. *Id.*

163. *See* Press Release, U.S. Dep't Treasury, *supra* note 3.

164. *See* Blackwell, *supra* note 18. For U.S. banks, officials estimate that both domestically and internationally there are 500 million wire transfers a year. *Id.*

165. *See* Kaper, *supra* note 145.

166. Stacy Kaper, *Agencies Criticize Idea of Reports on Wire Transfers*, AM. BANKER, June 21, 2006, at 3.

in the future.[167] Yet, FinCEN officials have been more elaborate in addressing other concerns.[168] For example, FinCEN officials have been quick to cite the importance of an all-international-wires-reporting requirement in furtherance of protecting economic and national security.[169] In addition to highlighting the security benefits of the proposal, FinCEN has attempted to calm the banking industry's concerns over the potential wide application of the new reporting requirement to banks of all sizes by implying that in all likelihood the reporting requirement will apply only to larger financial institutions that are regularly involved in international wire transactions.[170] Lastly, FinCEN officials have openly attempted to distinguish the new reporting proposal from SWIFT and SARs by arguing that the all-international-wires-reporting requirement is a supplement to areas of financial information not currently covered by SARs and other reports.[171] However, FinCEN's attempt to convince bankers that the reporting efforts of the SWIFT program are different than those of the new proposal appears, at first glance, to be unconvincing.[172] This lack of explanation can arguably be traced to the government's reluctance to expose even more details on the operation of the SWIFT program—a program that the government still uses and views as a valuable tool in the War on Terror.[173]

Overall, neither the banking industry nor FinCEN officials have offered detailed evidence in support of their respective assertions that the SWIFT reporting requirement and the FinCEN reporting requirement do or do not achieve the same end result.[174] Instead, the only definitive information that both parties seem to acknowledge is that the FinCEN proposal appears to have an

167. *See* Bruce, *supra* note 155.

168. *See, e.g., FinCEN Seeks Industry Input on Feasibility of Collection of Cross-Border Wire Transfer Data*, *supra* note 153.

169. *Id.*

170. *See* Bruce, *supra* note 155. Financial Crimes Enforcement Network Director Robert Werner said that if the FinCEN proposal is approved, "probably fewer than 100 U.S. institutions would be directly affected." *Id.*

171. *See id.*

172. *Id.* At a conference, FinCEN Director Robert Werner merely said that the "reporting effort[s]" under FinCEN would be different than those under SWIFT; ultimately declining to discuss specific questions about the SWIFT program. *Id.*

173. *See Hearing*, *supra* note 4.

174. *See* Adler, *supra* note 20; Bruce, *supra* note 155.

across-the-board requirement of reporting all international wire transactions regardless of the size of the transaction, the parties involved, and whether there is any relationship to terrorism.[175] On the other hand, as explained by the Treasury Department, the SWIFT program involves a much more narrow type of financial information which requires a suspected link to terrorism in order to access.[176]

VI. CONCLUSION

For over five years the U.S. government and the SWIFT cooperative maintained a secret arrangement[177] in which government officials had access to specific financial records stored in SWIFT's vast databases as long as SWIFT received a compulsory subpoena and the requested search was related to terrorism.[178] The U.S. government viewed this relationship as an essential tool in the War on Terror[179] that was both easily accessible and had proven results.[180] However, this secret relationship was exposed this past summer as various newspapers publicized stories relating to the arrangement.[181] While the purpose of the exposure was in all likelihood to address potential privacy concerns for U.S. citizens,[182] the reality is that the news articles opened the door and revealed current controversies involving the European Union, SWIFT, the U.S. banking industry, and the U.S. government.[183] Although each controversy involves an element of uncertainty, available evidence in each situation permits a likely prediction of future events.

One, while EU nations continue to criticize the SWIFT program,[184] the fact that they have not pursued nor do they plan to

175. *See* Adler, *supra* note 20; Blackwell, *supra* note 144; Bruce, *supra* note 155.
176. *See Hearing*, *supra* note 4.
177. *See supra* notes 49-52 and accompanying text.
178. *See supra* note 57 and accompanying text.
179. *See supra* notes 52-60 and accompanying text.
180. *See supra* note 123 and accompanying text.
181. *See* Meyer & Miller, *supra* note 12.
182. *See* Bruce, *supra* note 16.
183. *See supra* notes 13-22 and accompanying text.
184. *See supra* notes 69-71 and accompanying text.

pursue any legal action against SWIFT or the United States[185] supports the assertion that the United States will continue to present SWIFT officials with compulsory subpoenas and, consequently, SWIFT will continue to turn over financial information.[186]

Additionally, while SWIFT continues to face a difficult dilemma regarding which party's interests will prevail (the national security interests of the United States or the privacy concerns of the European Union), [187] it appears that SWIFT will continue to obey the compulsory subpoenas of the United States.[188]

And although there appears to be some lingering unsettlement over the legality of the SWIFT program and whether it violates personal privacy laws, U.S. government officials believe the program is an essential tool in the War on Terror and in all likelihood will continue to obtain specific financial information through the use of compulsory subpoenas. [189]

Lastly, while the exposure of the SWIFT program has given members of the banking industry evidence to claim that a current FinCEN proposal mandating that banks report all international wire transactions is unnecessary, [190] the revelation also highlights the tension between banks and law enforcement agencies relating to current reporting requirements.[191] While banks and FinCEN officials continue to argue over the effectiveness of current reporting requirements, FinCEN has given no indication that it plans to decrease the reporting requirements for banks in the near future.[192] If anything, it is possible that banks will have even greater reporting requirements if the FinCEN proposal is approved.[193] Thus, new reporting requirements on top of currently disputed mandates could spell trouble for the War on Terror—as banks continue to file more and more SARs and law enforcement

185. *See supra* notes 75-78 and accompanying text.
186. *See supra* notes 93-100 and accompanying text.
187. *See supra* notes 83-100 and accompanying text.
188. *See supra* notes 93-100 and accompanying text.
189. *See supra* notes 116-19, 124-27 and accompanying text.
190. *See supra* notes 162-65 and accompanying text.
191. *See supra* notes 135-49 and accompanying text.
192. *See supra* notes 147-48 and accompanying text.
193. *See supra* notes 150-76 and accompanying text.

agencies arguably struggle to properly analyze the data,[194] the potential for terrorists and their related financial activity could fall through the cracks.[195]

JEREMY S. SHRADER

194. *See supra* notes 163-65 and accompanying text.
195. *See supra* notes 143-49 and accompanying text.