Virtual Uncertainty: Developments in the Law of Electronic Payments and Financial Services

Sarah Jane Hughes
Indiana University Maurer School of Law, sjhughes@indiana.edu

Stephen T. Middlebrook
FSV Payment Services

Follow this and additional works at: https://www.repository.law.indiana.edu/facpub

Part of the Administrative Law Commons, and the Commercial Law Commons

Recommended Citation
Hughes, Sarah Jane and Middlebrook, Stephen T., "Virtual Uncertainty: Developments in the Law of Electronic Payments and Financial Services" (2013). Articles by Maurer Faculty. 2095.
https://www.repository.law.indiana.edu/facpub/2095
Virtual Uncertainty: Developments in the Law of Electronic Payments and Financial Services

By Stephen T. Middlebrook* and Sarah Jane Hughes**

I. INTRODUCTION

The past year has seen significant legal changes concerning electronic payments and financial services. Some have resolved ambiguity, while others have increased uncertainty for those operating in these areas. Part II of this survey covers developments relating to virtual currencies, undoubtedly the most controversial and significant area this year. Part III looks at the efforts of the Consumer Financial Protection Bureau ("CFPB") to tweak the cross-border remittance transfer rule that the 2012 survey discussed.1 Part IV reviews the CFPB's first use of its preemption authority in determinations that void parts of Tennessee's gift card escheat law,2 while leaving a similar Maine law3 in force.4 Part V briefly covers the first enforcement action by the Federal Deposit Insurance Corporation ("FDIC") against a bank for unsafe and unsound banking practices, unfair or deceptive practices, and more in connection with its prepaid card business.5 Part VI sets forth some conclusions about the manner in which the federal government appears to be approaching the regulation of e-payments and financial services.

* Stephen T. Middlebrook is the General Counsel of FSV Payment Systems, Inc., a prepaid processor and program manager. Prior to joining FSV, he was Senior Counsel at the U.S. Department of the Treasury, Financial Management Service. He is the current co-chair of the Electronic Payments and Financial Services Subcommittee of the Cyberspace Law Committee. He can be reached at stm@aol.com. The views contained in this survey are his and may not reflect the views of his employer.

** Sarah Jane Hughes is the University Scholar and Fellow in Commercial Law at the Maurer School of Law at Indiana University. She is a former co-chair of the Electronic Payments and Financial Services Subcommittee of the Cyberspace Law Committee and that Committee's current publications chair. She can be reached at sjhughes@indiana.edu. The views contained in this survey do not reflect the views of the Maurer School of Law or the Trustees of Indiana University.

5. See infra notes 79–87 and accompanying text.
II. RECENT DEVELOPMENTS IN THE REGULATION OF VIRTUAL CURRENCIES

The legal landscape for virtual currencies remained undisturbed from when we last wrote about the subject in 2008 until early 2013, when both regulators and law enforcement turned their attention to these alternative payment systems. Their actions were likely influenced by growing usage of virtual currencies, especially Bitcoin. The Financial Crimes Enforcement Network ("FinCEN") issued guidance clarifying the application of anti-money laundering rules to virtual currencies ("FinCEN Guidance"). That guidance was followed by two significant law enforcement actions. First, the Department of Homeland Security ("DHS") seized funds belonging to Mt. Gox, a major Bitcoin exchange. Shortly thereafter, the Department of Justice ("DOJ") indicted Liberty Reserve, a major international digital currency company, and its principals, on charges of money laundering.

Subpart A of this section evaluates the FinCEN Guidance. Subpart B covers DHS's seizure of Mt. Gox's funds; and Subpart C covers the DOJ's indictment of Liberty Reserve.

A. FINCEN ISSUES NEW GUIDANCE ON VIRTUAL CURRENCIES

On March 18, 2013, FinCEN issued interpretive guidance clarifying the application of the Bank Secrecy Act to virtual currencies. FinCEN had previously promulgated regulations governing money services businesses ("MSBs"), including currency exchanges and money transmitters, which are obligated to comply with registration, record-keeping, and other requirements ("MSB Rule"). This new guidance attempts to clarify if and when participants in virtual currency transactions might be engaging in "money transmission" and thus subject to the MSB Rule.

---


11. FinCEN Guidance, supra note 8, at 1.

FinCEN begins its guidance by distinguishing "real" currency from "virtual" currency. Real currency is the coin and paper money of the United States, or another country, that has the status of legal tender in the country of issue. Virtual currency does not have legal tender status and thus is not real currency. Some virtual currency, however, has an equivalent value in real currency or may be used as a "substitute" for real currency, and FinCEN deems this "convertible virtual currency." FinCEN is not explicit on this point, but presumably a virtual currency such as Bitcoin that can be exchanged for real currency would constitute a convertible virtual currency.

Because convertible forms of virtual currency may "substitute" for real currency, a transaction in these virtual currencies may qualify as a "money transmission." FinCEN defines "money transmission" as "the acceptance of currency, funds, or other value that substitutes for currency from one person and the transmission of currency, funds, or other value that substitutes for currency to another location or person by any means." Whether a particular entity is or is not a "money transmitter" is "a matter of facts and circumstances," but the rules set forth a number of specific exemptions. A person who takes a convertible virtual currency from one person and then transmits that convertible virtual currency to another person or location would be a "money transmitter," according to the FinCEN Guidance.

The FinCEN Guidance next divides participants in virtual currency arrangements into three categories: users, exchangers, and administrators. "Users" obtain virtual currency in order to purchase real or virtual goods and services. "Exchangers" engage in the exchange of virtual currency for real or virtual currency as a business. "Administrators" engage in the business of issuing and redeeming virtual currency. Users are not MSBs because they do not transmit the value of funds to another person or location. An exchanger or administrator will be a "money transmitter" if it (1) accepts and transmits a convertible virtual currency between persons or from one location to another, or (2) buys or sells convertible virtual currency, unless, in either case, an exemption applies. An intermediary that accepts and transmits funds solely for the purpose of completing a bona fide purchase or sale of currency—real or virtual—is exempt and will not be treated as a "money transmitter." However, FinCEN views an

13. FinCEN Guidance, supra note 8, at 1.
14. Id.
15. 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2013) (defining "money transmission services").
16. Id. § 1010.100(ff)(5)(i)(B)(ii).
17. FinCEN Guidance, supra note 8, at 3.
18. Id. at 2.
19. Id.
20. Id.
21. Id.
22. Id.
23. Id. at 4.
24. Id. at 3.
25. Id.
exchange that takes funds from a user and then transmits those funds to the user’s account at the administrator to be engaged in “money transmission.”

In a virtual currency system such as Bitcoin, which operates without a central administrator, a person who creates units of the virtual currency (a “miner” in Bitcoin parlance) and uses it to purchase real or virtual goods is merely a user and would not be a “money transmitter.” In contrast, FinCEN clarifies that “a person that creates units of convertible virtual currency and sells those units to another person for real currency or its equivalent is engaged in transmission to another location and is a money transmitter.” Thus, a Bitcoin “miner” who creates and sells Bitcoins for real currency is apparently a “money transmitter.” However, FinCEN’s definitions of both an “exchanger” and an “administrator” contain the phrase “engaged as a business,” which is not defined. It is unclear at what point an entity participating in the virtual currency market would be deemed to be “engaged as a business,” and thus it is difficult to advise when the MSB Rule begins to apply.

While the FinCEN Guidance does not specifically reference Bitcoin, the applicable rules have drawn criticism from Bitcoin proponents. For example, Patrick Murck, legal counsel for the Bitcoin Foundation that promotes use of the virtual currency, said that the FinCEN Guidance “would be infeasible for many, if not most, members of the Bitcoin community to comply with.” At least three “exchanges” that traded Bitcoins shut down shortly after the new guidance was issued. Treasury Undersecretary David Cohen stated that virtual currency exchanges that comply with the law “have nothing to fear from Treasury.”

Given compliance challenges, however, those exchanges are unlikely to find much comfort in Cohen’s statement.

B. HOMELAND SECURITY SEIZES FUNDS HELD BY BITCOIN EXCHANGE MT. GOX

On May 14, 2013, DHS obtained a seizure warrant directed to Dwolla, an Iowa-based internet payments company, ordering the seizure and forfeiture of an account belonging to Mutum Sigillum, LLC. According to the affidavit of

26. See id. at 4.
27. See id. at 5. How one obtains virtual currency may be described using various terms—such as “mining”—depending on the specific virtual currency model. See id. at 2 n.7.
28. Id. at 5.
29. Id. at 2.
a federal agent filed with the warrant application, Mutum Sigillum is the U.S.-based subsidiary of Mt. Gox, which is the world's largest Bitcoin exchange and which is based in Japan. The affidavit stated that a confidential informant residing in Maryland established an account at Dwolla that he used to fund an account at Mt. Gox and to purchase Bitcoins. In addition, the informant also exchanged Bitcoins for U.S. dollars that were transmitted back to him through Mutum Sigillum and Dwolla accounts. Apparently relying upon, but not citing to, the FinCEN Guidance, DHS asserted that those transactions demonstrated that Mutum Sigillum was engaged in "money transmission." The affidavit noted that Mutum Sigillum was not registered with FinCEN as required by 31 U.S.C. § 5330, and asserted that Mt. Gox consequently was in violation of 18 U.S.C. § 1960 and subject to legal penalties. One such penalty is the forfeiture of property as authorized by 18 U.S.C. § 981(a)(1)(A). The affidavit noted that Mutum Sigillum funds were also transmitted through an account at Wells Fargo and that a separate warrant was issued to seize funds in that account. While law enforcement executed warrants to seize the funds of Mt. Gox located in the United States, as of June 12, 2013, no indictments of Mt. Gox or its subsidiary Mutum Sigillum have been handed down. Mt. Gox subsequently implemented a new policy requiring identity verification before it would perform currency deposits or withdrawals.

C. DEPARTMENT OF JUSTICE INDICTS LIBERTY RESERVE FOR MONEY LAUNDERING


35. Id. at 3.
36. Id.
37. Id.
38. Id. at 1–2.
39. Id. at 4–5.
40. Id. at 4; see also Brian Browdie, Bitcoin Exchange in U.S. Crosshairs Banked at Wells Fargo, AM. BANKER (May 16, 2013, 8:43 AM), http://www.americanbanker.com/issues/178_95/Bitcoin-exchange-in-u-s-crosshairs-banked-at-wells-fargo-1059158-1.html.
were also charged with conspiracy to commit money laundering in violation of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1956(a)(2)(B)(i). Liberty Reserve is alleged to have been a “financial hub of the cyber-crime world, facilitating . . . credit card fraud, identity theft, investment fraud, computer hacking, child pornography, and narcotics trafficking.” The government estimated that Liberty Reserve had 200,000 users in the United States and processed over twelve million transactions a year with a value of more than $1.4 billion.

Allegedly, Liberty Reserve did not require users to validate their identity, and criminals created accounts under false names such as “Russian Hackers.” The government alleges that Liberty Reserve, in an effort to add an additional layer of anonymity, did not permit users to transmit funds directly to Liberty Reserve, but instead required them to make deposits and withdrawals through third-party exchanges. Liberty Reserve allegedly recommended third-party exchanges that tended to be unlicensed money transmitters operating without government oversight and that were concentrated in Malaysia, Russia, Nigeria, and Vietnam. Pursuant to 18 U.S.C. § 982(a)(1), the government seeks forfeiture of “at least $6 billion” held in accounts in Costa Rica, Cyprus, Russia, Hong Kong, China, Morocco, Spain, Latvia, and Australia, as well as one account at SunTrust Bank in the United States.

Of special interest to followers of cyberspace law, in a declaration filed in support of a post-indictment restraining order, seizure warrant, and injunction against Liberty Reserve, a Secret Service agent stated that the investigation included execution of “one of the first-ever ‘cloud’-based search warrants, directed to a service provider used to process Liberty Reserve’s Internet traffic.” The government also sought an injunction preventing Amazon Web Services from providing services to support Liberty Reserve’s website.

On the same day that indictment was unsealed, FinCEN issued a notice of proposed rulemaking to declare Liberty Reserve an institution of primary money laundering concern under section 311 of the Patriot Act. The rule would prohibit all U.S. financial institutions from maintaining correspondent relationships with foreign banks that do business with Liberty Reserve.

%20et%20al.%20indictment%20-%20Redacted.pdf. The charges also include conspiracy to operate an unlicensed money transmitter business. Id. ¶¶ 1-32.

44. Id. ¶¶ 1-32.
45. Id. ¶ 9.
46. Id. ¶ 10.
47. Id. ¶¶ 14 & 19.
48. Id. ¶ 16.
49. Id. ¶ 18.
50. Id. ¶ 43.
52. Id. ¶ 74.
54. See id. at 34009.
The measure would effectively cut off Liberty Reserve from the U.S. financial system. While the Mt. Gox forfeiture order and the Liberty Reserve criminal indictment are quite different on a number of levels, both use 18 U.S.C. § 1960 to enforce the registration requirement for MSBs with severe penalties, including asset forfeiture and additional criminal sanctions. Prosecutors employed essentially the same strategy against e-Gold, which we described and critiqued in prior surveys. These actions, following so soon after the publication of the FinCEN Guidance, signal the government’s intent to police the virtual currency market robustly. These methods may be a convenient and effective way for law enforcement to deal with money launderers, but they have potentially significant collateral effects on small companies and start-ups that wish to operate within the confines of the law, but lack the resources or the expertise to navigate such tricky regulatory waters. Establishing appropriate compliance obligations without stifling innovation in emerging payments technology is always a concern. With regard to virtual currencies, it remains to be seen whether the government has found the proper balance.

III. The CFPB Tweaks and Re-Tweaks the “Remittance Transfer” Rule

Responding to industry concerns, the CFPB has tweaked its February 2012 rule amending Regulation E ("2012 Remittance Rule") to implement the cross-border remittance transfer provisions of Dodd-Frank Act's section 1073 on several occasions. On May 22, 2013, the CFPB amended the 2012 Remittance


Rule in three major respects. These May 2013 amendments (1) permit disclosure of fees imposed and taxes to be collected by any person other than the remittance transfer provider; (2) require disclaimers indicating that the recipient may receive less than the disclosed total, due to the fees and taxes for which disclosure is now optional; and (3) exempt transactions from the error provision requirements if funds are deposited into an account other than that of the intended recipient because the consumer-sender supplied an incorrect account number or recipient institution identifier.

IV. THE CFPB PREEMPTS GIFT CARD ESHEAT LAWS IN TENNESSEE BUT NOT MAINE

The Credit Card Accountability Responsibility and Disclosure Act of 2009 ("Credit CARD Act") amended the Electronic Fund Transfer Act ("EFTA"), among other things, to prohibit expiry of funds underlying gift cards before the later of five years from the date of initial issuance of the card or the date of the last funds loaded onto the card. The EFTA preempts state laws only to the extent of inconsistency with its provisions, unless the state law is more protective of consumers.

Many states require escheat of unused and dormant balances on gift cards as quickly as two years after issuance or the last value is added to the card.
These escheat laws conflict with the Credit CARD Act if, after remitting unused balances to the state, issuers refuse to honor cards. In April 2013, the CFPB determined that the EFTA preempted section 66-29-116 of Tennessee’s Uniform Disposition of Unclaimed Property Act because that section allowed issuers to decline to honor cards as soon as two years after issuance and relieved them of liability to consumers. The CFPB concluded that Tennessee’s law “permit[s] cards and their underlying funds to expire sooner than is permitted under the EFTA and Regulation E.”

Maine similarly relieves gift card issuers from liability to card owners after issuers transfer underlying funds to the State. The CFPB, however, did not preempt Maine’s statute, relying on “communications” with the Office of the State Treasurer (“Maine’s Treasurer”) that it instructs gift card issuers who transfer unclaimed funds to the State to honor cards on subsequent presentation “indefinitely” and then to request reimbursement from the State. Maine’s Treasurer apparently persuaded the CFPB that its consumers could use their gift cards for at least as long as they are guaranteed that right by the EFTA and Regulation E. Commentators described the CFPB’s rationale for not preempting Maine’s law as “novel” or used words of similar import.

Those commentators criticized the CFPB’s position that issuers who honor cards should look to the state for reimbursement of abandoned funds previously transferred to the state. Some commentators observed that card issuers will be

---

68. Tenn. Code Ann. § 66-29-135(a) (2004) (providing that card is presumed abandoned if unclaimed two years from issuance); id. § 66-29-116 (“Any person who pays or delivers abandoned property to the treasury ... is relieved of all liability ... which thereafter may arise ... in respect of the property.”). For discussion of the CFPB’s view of Tennessee’s law pertaining to cards that cannot be used at multiple, unaffiliated merchants or at automated teller machines, see Electronic Fund Transfers; Determination of Effect on State Laws (Maine and Tennessee), 78 Fed. Reg. at 24390.


70. Id. at 24391; see also 12 C.F.R. § 1005.20(e)(2)(i) (2013) (prohibiting expiry in less than five years).


73. Id. at 24389-90.

74. Id. at 24390.


77. See Fischer, Poindexter, Chamin & Janiga, supra note 75, at 3; Strahlberg & Rinearson, supra note 76, at 2.
required to pay "twice the value of funds . . . loaded"—once to the state and again to the card holder—and then seek reimbursement from the state.78

V. THE FDIC'S ENFORCEMENT OF TREASURY'S "FEDERAL BENEFITS" RULE EXTENDS REGULATION E'S PAYROLL CARD PROVISIONS TO GENERAL PURPOSE PREPAID CARDS THAT CONTAIN FEDERAL BENEFITS

On May 31, 2013, the FDIC announced settlements with a bank and an affiliated prepaid card issuer for violations of the Treasury Rule, 31 C.F.R. § 210, which governs the use of the Automated Clearing House system to deliver federal benefit payments to prepaid debit cards.79 The FDIC determined that First California Bank ("FCB") and its institution-affiliate, Achieve Financial Services, LLC ("Achieve"), engaged in unfair and deceptive practices in the marketing and servicing of a prepaid, reloadable credit card.80 The consent orders require FCB and Achieve to comply with the Treasury Rule (including protections afforded by Regulation E),81 the guidance offered by the FDIC and the Federal Reserve regarding unfair or deceptive practices,82 and section 5 of the Federal Trade Commission Act,83 and also to implement extensive auditing and compliance programs.84 FCB agreed to pay a civil penalty of $600,000 to the FDIC and to oversee (and effectively guarantee) restitution of $1,110,000 for consumers who used prepaid products marketed by two card issuers.86 The consent orders effectively establish Regulation E's rules for "payroll cards" as the standard for general-purpose reloadable ("GPR") cards.87 As a result, it may reduce the...
need for CFPB regulations related to GPR cards. It also is the first occasion of which we are aware that an issuer of prepaid cards—FCB—has been pursued for the faults of its third-party program manager.

VI. CONCLUSION

Despite attempts at clarification, many ambiguities remain following the FinCEN Guidance on virtual currencies and the application of the MSB Rule, as discussed in Part II. In addition to the FinCEN Guidance, virtual currency providers are also facing potential regulation from the Commodity Futures Trading Commission and from the states. These new regulations will add to compliance burdens and present new challenges to these emerging businesses. Prepaid card businesses also will continue to face uncertainty as they try to unravel the limits of the preemption authority of the CFPB under the Credit CARD Act, as discussed in Part IV.

Greater certainty will flow from other 2013 actions by the federal government, including publication of the final rule titled Garnishment of Accounts Containing Federal Benefit Payments, the May 2013 amendments to CFPB’s remittance transfer rule described in Part III, and from application of the Treasury Rule and Regulation E’s “payroll card” provisions to federal benefits paid via prepaid cards discussed in Part V.

90. See supra notes 63–78 and accompanying text.
92. See supra notes 57–62 and accompanying text.
93. See supra notes 79–87 and accompanying text.