Privacy and Data Security and Virtual Currencies: A Complex of Domestic and Foreign Compliance Standards and Issues to Consider

BY SARAH JANE HUGHES

I. Introduction

Price volatility has been a major focus of followers of virtual currencies since September, as the value of bitcoin and other virtual currencies first tumbled and then recovered in part. Price volatility, however, is but one of five obstacles to the progress of virtual currencies into a more mainstream position in the domestic and global economy.

This article looks at three of the other four obstacles—privacy and security concerns and building the general public’s trust in virtual currencies and market participants. Privacy and security are vital to building and maintaining confidence in both virtual currencies and the exchanges and wallet providers that enable users to complete payments transactions with them. The last obstacle—the general issue of whether government regulation of virtual currency market participants is needed for broader acceptance of virtual currencies—is being addressed in other venues.

After some background on privacy and security issues affecting virtual currencies, this article explains how privacy and security concerns affect transactions settled in virtual currencies and describes the growing complex of laws and regulations with which market participants should be fully acquainted, as well as new initiatives that pertain to privacy and security. It closes with some advice for users.

II. Basic Considerations Relating to Privacy and Security in Virtual Currency Transactions

One of the major perceived benefits from math-based currencies such as bitcoin is the notion that users’ identities can be protected from those who could exploit that information for commercial purposes or to perpetrate identity theft. Other users may prefer to make it harder for government agencies to follow their transactions, whether on- or offline, a variant of the right to be left alone. To persons and firms so inclined, math-based currencies have many of the best attributes of cash in that they are perceived as anonymous exchanges.

Additionally, math-based currencies do not rely on governments for their creation or value, and do not require the use of intermediaries such as banks and currency exchanges for transactions involving distances and cross-currency transactions. They also offer a means of avoiding fees that intermediaries may charge. Of equal or perhaps greater importance, some argue, the payments may occur much faster and on a more predictable timetable than payments made through the

---

Sarah Jane Hughes is a university scholar and fellow in commercial law at Indiana University Maurer School of Law. She is a nationally recognized expert on payment systems; public and private methods to deter, detect and prosecute domestic and international money laundering; and consumer protection and financial privacy.
use of legacy correspondent banking, wire transfer and remittance transfer systems. Proponents of virtual currencies as methods of payment may believe that some of the data-gathering and management issues that have hounded Internet-based transactions as well as mobile payments do not apply to math-based currency transactions. However, for many transactions, particularly those in which a user buys tangible goods such as a product sold by Dell Inc. or Overstock.com Inc. or services from Dish Network or a local dentist or lawyer, the same transactional privacy concerns will apply. Some databases used by the seller and the shipper the selector, at the least, will hold information about the buyer’s whereabouts and the nature of the purchase.

Math-based currency users will reassure themselves that, surely, even if the real-world portion of the transaction has some privacy and security issues, the payment portion of the transaction will enjoy more privacy and more security than a payment made using a more traditional payment method or provider. And here lies a privacy fallacy about virtual and math-based currency payments. However much users want to believe that math-based currency payments will be more private than currently available payments methods and providers, in part because fewer intermediaries may be involved, users must deal with—and their counter-parties must decide how to manage—the fact that most payments made with math-based currencies for real-world transactions in goods and services will involve other participants and potentially the same or similar types of participants or as many participants as those using more traditional methods and providers.

Unless market participants adopt and observe strong privacy protocols and can control their agents via contractual restrictions on reuse, many of the same impulses to collect and reuse the data about the purchase of goods or services will remain. Moreover, whenever more participants are involved in any transaction, regardless of whether they play a role in the purchase or delivery of goods or the payment portion, the greater the risk that the private information about the purchaser/user will be compromised and reused without permission. This means that the privacy of the user’s information from the transaction is only as solid as the privacy protocols in effect at the weakest link in the transaction, which is likely to be the consumer herself, the retailer or service provider or the processor hired by the retailer or service provider.

Similar assumptions—and, I think, similar or larger-sized fallacies—apply to security issues that surround Internet-based transactions, and virtual or math-based currency payments. The “block chain”—the shared registry that records and confirms the existence of a mined bitcoin and that tracks transfers of ownership of bitcoins or fractional interests in them—is itself secured by strong algorithms. But the intermediaries—the providers of wallet services and exchanges and individuals’ communications with them—appear to be vulnerable to hacking, including “transaction malleability concerns.” Moreover, the larger the merchant or payments intermediary involved, the more attractive that user’s databases will be to hackers, as recent revelations about payments data security breaches involving legacy payments products demonstrate.

III. What Privacy Regulations Apply to Transactions Paid for Using Virtual Currencies?

The temptation for retailers and others dealing with new technologies is to be caught up in what I call “the Wild West syndrome,” the belief that preexisting regulations do not apply to their operations. In the case of transactions settled with virtual currencies, the same privacy rules that apply to retailers and depository and non-depository providers of consumer financial services apply.


5 Bitcoin, How Bitcoin Works, available at https://bitcoin.org/en/how-it-works. Bitcoin’s explanation of the block chain is that it is “a shared public ledger on which the entire bitcoin network relies. All confirmed transactions are included in the block chain. This way, bitcoin wallets can calculate their spendable balance and new transactions can be verified to be spending bitcoins that are actually owned by the spender. The integrity and the chronological order of the block chain are enforced with cryptography.” Id. (emphasis in original).

6 See Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 5–6, available at https://bitcoin.org/bitcoin.pdf; see also Bitcoin, Frequently Asked Questions, https://bitcoin.org/en/faq#security (explaining the security features embedded in bitcoin transactions, and the solution to the verification of the spending of that bitcoin or fraction of it to solve the “double-spending problem” that the system was in part designed to correct).

A. What Privacy Regulations Apply if the Transaction Includes a Consumer Customer Resident in the U.S.?

1. Dedicated Privacy Statutes and Regulations

In the U.S., 47 states, the District of Columbia, Guam, Puerto Rico and the U.S. Virgin Islands have dedicated privacy laws that apply to retailers and others.10 Also, Title V of the Gramm-Leach-Bliley Financial Services Modernization Act of 1999 (GLB Act) governs collection and opportunities for depository and non-depository providers of consumer financial services to share non-public personally identifiable information they receive in the course of consumers applying for financial services or in the management of the account by the provider.11 Finally, the federal Fair Credit Reporting Act,12 together with the federal regulations that implement both Title V13 and the FCRA,14 apply to depository and non-depository providers and retailers that offer credit.

2. More Generic Unfair or Deceptive Acts or Practices Authority

An additional source of privacy regulation in the U.S., but one perhaps less obvious to smaller retailers and newcomers, is Section 5 of the Federal Trade Commission Act,15 companion authority granted to the Consumer Financial Protection Bureau (CFPB) and federal bank regulatory agencies16 and the “little FTC Acts” that many states enacted.17 Section 5 of the FTC Act proscribes unfair methods of competition and, more pertinently for this audience, unfair or deceptive acts or practices in commerce.18 More than two decades ago, the FTC issued formal policy statements outlining its views on the proper exercise of its “unfairness” and “deceptive practices” authorities.19

Two recent enforcement actions by the FTC demonstrate the reach of its “unfair or deceptive acts or practices” powers. The first was brought against Wyndham Worldwide Corp., the parent of Wyndham hotels and affiliated hotel chains,20 and shows the FTC’s powers over retailers and others and why two privacy and security commentators have called the FTC the “most influential privacy and data security regulator in the United States.”21 The FTC charged that, in addition to failing to protect the personally identifiable information of its customers, Wyndham promised that it followed “standard industry practices” and also utilized other precautions to protect consumers from loss; in fact, the FTC alleged, not only did it not do as it claimed, Wyndham’s practices caused fraud losses to consumers of more than $10 million.22 The U.S. District Court for the District of New Jersey rejected Wyndham’s three claims: (1) that the FTC lacked authority under its Section 5 “unfairness” powers to regulate data security; (2) that the agency had not provided sufficient guidance for businesses as to what it would consider unfair practices in the data security field; and (3) that the FTC should have promulgated regulations before embarking on enforcement actions.23

The second involved a firm called LabMD Inc., a medical testing laboratory, which challenged the FTC’s

---

13 16 C.F.R. pt. 313 (2011) (Federal Trade Commission regulations requiring recipients of consumers’ personally identifiable information to safeguard it while in their possession or control).
16 12 U.S.C. §§ 5531 and 5536 (unfair, deceptive or abusive acts or practices). For the agencies’ relevant enforcement authorities, see 12 U.S.C. §§ 1786(e), 1786(k)(2), 1818(b), 1818(i)(2), 5531, 5536 and 5561-5566. The CFPB’s authority to issue regulations governing unfair, deceptive or abusive acts or practices is codified at 12 U.S.C. § 5531(b).

---

FTC acts, this excellent piece cites specific examples of enforcement actions related to health-care providers brought by various states using this authority that will assist readers in evaluating how the states in which they do business are likely to view certain conduct.).
22 First Amended Complaint, supra note 20.
authority to conduct an investigation of the firm’s security practices.24 The FTC’s original 2013 administrative complaint against LabMD alleged that the firm had not “reasonably protected the security of consumers’ personal data, including medical information.”25 The complaint alleged that in two separate incidents, LabMD collectively exposed the personal health information of approximately 10,000 consumers. The FTC’s complaint alleged that LabMD billing information for over 9,000 consumers was found on a peer-to-peer file-sharing network and then, in 2012, LabMD documents containing sensitive personal information of at least 500 consumers were found in the hands of identity thieves. The FTC explained that its action against LabMD is part of the FTC’s “ongoing effort . . . to ensure that companies take reasonable and appropriate measures to protect consumers’ personal data.”26 LabMD filed a motion with the FTC to dismiss the administrative complaint, and following the FTC’s denial of that motion, it filed an action in the U.S. District Court for the Northern District of Georgia for an injunction against further agency action in the U.S. District Court for the Northern District of Georgia for an injunction against further agency proceedings on the grounds that the agency lacked statutory authority to address the data security practices of companies to which the Health Insurance Portability and Accountability Act of 1996 (HIPAA)27 applies and that application of the FTC statute to LabMD would violate the Due Process Clause. The district court denied the preliminary injunction,28 and LabMD appealed to the U.S. Court of Appeals for the Eleventh Circuit, which has decided to hold oral argument on the issue raised.29 One of the more important issues is whether Section 5 rounds out the privacy and data security responsibilities under otherwise specifically targeted statutes such as HIPAA, or whether the presence of a dedicated federal privacy statute such as HIPAA occupies the field leaving no room for Section 5 jurisdiction.

B. What Privacy Regulations Apply if a Transaction Involves a Consumer Customer Resident Outside the U.S.?

For retailers as well as virtual currency exchanges and wallets, a key concern is identifying each law that might apply to any customer, based on the jurisdiction in which the consumer customer resides. These laws can vary significantly from those in effect in the U.S. For example, in Canada, where presumably many retailers in the U.S. have online customers, applicable laws include the Personal Information Protection and Electronic Documents Act (PIPEDA)30 and laws enacted by the provincial governments.31 In the European Union, applicable laws include the 1995 Data Protection Directive (95/46/EC).32

Compliance responsibilities for the protection of consumers’ personal information are increasing in Japan and the Asia-Pacific Economic Cooperation (APEC) countries. In Japan, for example, the Data Protection Act was enacted in 2003 and became effective April 1, 2005.33 The Japanese government, late in 2013, announced its intention to prepare amendments to the act for introduction in June 2014. Also, the Ministry of Economy, Trade and Industry (METI) published a code on privacy notices that includes a checklist of what should appear in all consumer privacy notices, including the following disclosures that go beyond those required by the FTC regulations implementing the GLB Act’s Title V, particularly:

- the process of data collection, as well as the nature of the personal data collected;
- the explanations of the consumers’ right to object to collection of their data, and of their rights to have data corrected and the process for exercising such rights; and
- the period of time that the collector will retain the data, and information explaining the manner in which the data will be destroyed at the end of that period.34


31 British Columbia (Personal Privacy Protection Act, [SBC 2003] CHAPTER 63), Alberta (Personal Privacy Protection Act, ch. P-6.5) and Quebec (Act respecting the protection of personal information in the private sector, ch. P-39.1) have their own privacy legislation that supersedes PIPEDA, but the other seven provinces and three territories in Canada follow PIPEDA. See Canadian Privacy Legislation, PrivacySense.net (2014), available at http://www.privacysense.net/privacy-legislation/canadian/.


The METI code also calls for standardized and clear notices to avoid consumer confusion.35

Australia enacted its Privacy Act in 198836 and implemented its Privacy Principles in March 2014.37 Mexico, the U.S. and Japan qualified for APEC’s Cross Border Privacy Rules (CBPR) System implementation.38

Requirements of privacy laws in the U.S., Canada, the EU and the APEC nations vary. Some carry the prospect of penalties as well as restitution for losses or other redress. Accordingly, retailers and payments processors working with retailers need to ascertain the country of residence of any consumers with whom they are dealing or whose personally identifiable information they collect or maintain as part of their role in the transaction. Only by identifying the residence of the consumer customer can the seller of goods or services be certain that the seller can apply the proper privacy protections to the particular transaction. The fact that the consumer pays for the purchase using a virtual currency does not alter this basic responsibility to identify the governing privacy law and to comply with its requirements.

IV. What Additional Security Regulations Apply to Virtual Currency Transactions?

Many businesses that take payments in a form of virtual currency will already be familiar with any existing payments security regulations and system requirements that apply in their country. In the U.S., only a handful of states have data security laws.39 So, for the most part, data security is a function of federal law, including the GLB Act’s Title V and the FTC’s Safeguards and Disposal Rules, which require that persons and entities holding personal information adopt physical, administrative and technical procedures to safeguard and to dispose safely of the personal information.40 An additional source of federal standards for privacy and data security is HIPAA, whose Title V requires health-care providers and others to implement both privacy and security procedures that also have to employ physical, administrative and technical safeguards for personal information.41

So, these businesses should acquaint themselves with two of the most formidable changes that are likely to affect their businesses in the near future—the forthcoming EU Network & Information Security Directive42 and the proposed cybersecurity provision of the New York State Department of Financial Services (DFS) Virtual Currency Regulatory Framework (the BitLicense proposal).43

For the purposes of this article, I will focus on two aspects of the BitLicense proposal that bear on data security and privacy. First, the proposal includes an anti-money laundering program requirement that will require capture and retention of specific personal information, require verification of customers’ identities, impose enhanced requirements on foreign accounts and prohibit business with shell corporations.44 Second, and of greater potential significance to the body of data security laws that apply to virtual currencies, it contains a dedicated cybersecurity requirement.45 Two features of the cybersecurity requirement deserve special attention as retailers and others develop their plans to comply with the DFS BitLicense proposal. Persons and entities qualifying as “virtual currency market participants” will have to develop and implement programs that fulfill “five core functions”:

1. identify internal and external cyber risks by, at a minimum, identifying the information stored on the Licensee’s systems, the sensitivity of such information, and how and by whom such information may be accessed;

2. protect the Licensee’s electronic systems, and the information stored on those systems, from unauthorized access, use, or other malicious acts through the use of defensive infrastructure and the implementation of policies and procedures;

3. detect systems intrusions, data breaches, unauthorized access to systems or information, malware, and other Cyber Security Events;

4. respond to detected Cyber Security Events to mitigate any negative effects; and

5. recover from Cyber Security Events and restore normal operations and services.46

And, they must develop and implement a cybersecurity policy that covers 13 aspects of their use of virtual currencies:

1. information security;

2. data governance and classification;

3. identify and mitigate the following risks:

   a. unauthorized access to data;
   b. data manipulation;
   c. denial-of-service attacks;
   d. theft of data;
   e. data loss; and
   f. tampering.

4. (1) implement and maintain systems and network security measures to protect the confidentiality, integrity and availability of information and systems; (2) protect the Licensee’s electronic systems, and the information stored on those systems, from unauthorized access, use, or other malicious acts through the use of defensive infrastructure and the implementation of policies and procedures; (3) detect and respond to detected Cyber Security Events to mitigate any negative effects; and (4) recover from Cyber Security Events and restore normal operations and services.


45 Id. at § 200.15(g).

46 Id. at § 200.16.

47 Id. at § 200.16(a).
(3) access controls;
(4) business continuity and disaster recovery planning and resources;
(5) capacity and performance planning;
(6) systems operations and availability concerns;
(7) systems and network security;
(8) systems and application development and quality assurance;
(9) physical security and environmental controls;
(10) customer data privacy;
(11) vendor and third-party service provider management;
(12) monitoring and implementing changes to core protocols not directly controlled by the Licensee, as applicable; and
(13) incident response.47

Beyond these proposed requirements is a New York State DFS plan, announced in September, to focus its enforcement energies for the coming year on cybersecurity.48 One could assume that this announcement is designed to prompt financial institutions to adopt stronger security procedures to help guard against the hacking incidents mentioned above.49 But, given the aggressive stance that the DFS has taken generally, this announcement may signal that the DFS may take an approach to cybersecurity similar to the FTC’s in its enforcement actions against Wyndham and LabMD described above.50

V. How Can Virtual Currency Market Participants Ensure Their Compliance With Current and Future Privacy and Data Security Obligations in Jurisdictions in Which Their Customers Reside?

As a starting point, virtual currency market participants should look at the following five steps and prepare to follow developments in varied jurisdictions as their cross-border customer bases and transactions expand. Virtual currency market participants—retailers and payment services providers—should:

1. Know their customers and identify those who are consumers and where those consumers reside. This will allow participants to consult any requirements that may be applicable to that customer’s privacy and data security rights. Be prepared to verify customers’ identities, such as the DFS BitLicense proposal may require.

2. Appreciate the complex mix of domestic and international standards, including International Standards Organization standards, such as ISO 27018, that applies to certain aspects of housing personally identifiable information on behalf of others and in a public cloud. These domestic standards may include federal laws and regulations, state laws and unfair or deceptive acts or practices authority in Section 5 of the FTC Act and in state “little FTC Acts.” International standards include the Data Protection Directive, PIPEDA, the APEC’s CBPR System and the national regulations adopted in countries such as Australia and Japan.

3. Follow reports of data security breaches, particularly those affecting retailers and depository and non-depository providers of financial services, review data security and privacy protection procedures, including all administrative, technical and physical protections participants have employed, make changes according to changing threat levels and known vulnerabilities and periodically test the firm’s ability to respond to breaches in accordance with the laws applicable to your business. Make needed changes to all protocols and hardware in the event the business suffers a breach.

4. Follow proposed changes to federal and state laws that deal with the privacy of personally identifiable information or data security, consult with legal and compliance advisers on these aspects of the business and determine how to adjust administrative, technical and physical protocols to comply with emerging requirements.

5. Review any promises made to consumers on the firm’s website and make adjustments as needed to avoid enforcement actions such as those brought by the FTC against Wyndham and LabMD.

Beyond these steps, each firm that takes virtual currencies or other electronic forms of payment should follow changes in laws beyond privacy- and data security-centric laws, such as laws governing consumer payments domestically or across borders, anti-money-laundering laws and applicable economic sanctions programs to ensure overall compliance of their firms with all applicable laws.

47 Id. at § 200.16(b).
49 See supra note 9.
50 See supra notes 20 to 25.
SAFE DATA & SOUND SOLUTIONS

Privacy & Data Security Law Resource Center™

Unparalleled news. Expert analysis from the new Privacy & Data Security Portfolio Practice Series. Comprehensive new treatises. Proprietary practice tools. State, federal, and international primary sources. The all-in-one research solution that today’s professionals trust to navigate and stay in compliance with the maze of evolving privacy and data security laws.

TO START YOUR FREE TRIAL
CALL 800.372.1033 OR
GO TO www.bna.com/privacy-insights