



Paul Sieminski
General Counsel
Automattic Inc.
132 Hawthorne Street
San Francisco, CA 94107
[REDACTED]

March 27, 2015

Benjamin M. Lawsky, Superintendent of Financial Services
Dana V. Syracuse, Office of General Counsel,
New York Department of Financial Services
One State Street, New York, NY 10004-1511
Email: dana.syracuse@dfs.ny.gov

Re: Reply Comments on Proposed Rulemaking regarding Regulation of the Conduct of Virtual Currency Businesses - DFS-29-14-00015-P

Dear Mr. Lawsky,

I am writing on behalf of Automattic Inc. We are best known for operating the popular WordPress.com blogging and publishing platform. Our company's mission is to democratize publishing. We pride ourselves on promoting and powering speech on the Internet for publishers of all sizes, and have more than 77 million sites in our network. Sites running on our WordPress.com platform range from small blogs to large media properties like CNN, the New York Post, Time, USA Today and NBC Sports, as well as the corporate blogs of a number of Fortune 500 companies.¹

Automattic accepted bitcoin as payment for our paid WordPress.com upgrades from November 2012 – February 2015 (we recently paused bitcoin support due to resource constraints). When we began supporting bitcoin we noted that Paypal blocks payments in 60 countries, and other payments systems have similar restrictions, sometimes for political reasons.² We strongly support the open, decentralized principles behind the blockchain and digital currencies like bitcoin,

¹ Clients, WORDPRESS.COM VIP, <https://vip.wordpress.com/clients/>

² Andy Skelton, *Pay Another Way*, WORDPRESS.COM BLOG, Nov. 12, 2012, <http://en.blog.wordpress.com/2012/11/15/pay-another-way-bitcoin/>

and think they will play a major role in the future of commerce. Our CEO has said that he believes bitcoin “or some other blockchain-like system will be the basis of the majority of financial transactions in the future, from small remittances to multi-billion dollar corporate acquisitions.”³ For these reasons, we thought it was important to weigh in on the Department’s proposed regulations, which, as drafted, pose a significant risk to the future of digital currencies, not to mention the many other innovations that the technology underlying bitcoin has the ability to unleash down the road. Your revised proposal would pose a grave threat to innovation, entrepreneurship, and freedom of expression online.

While many of the corporate filers in this proceeding are directly involved in monetary transmission (of some sort) or run gift card programs, we come to this proposal as an Internet company and free-speech platform that has come to appreciate the legal and regulatory framework necessary for entrepreneurship and speech to flourish online. Based on our company mission, we believe in anonymous speech and in the innovative power of small independent developers and entrepreneurs using free, open source tools to build new businesses.

While we do not question the proposal’s good intentions, we are deeply concerned about its likely consequences. This proposal would create added costs and uncertainty that would outweigh any hoped-for benefits. If such rules are adopted, they should be thoughtfully considered at the federal – not the state – level to ensure national uniformity. The cybersecurity provisions are ill-informed and dangerous, and there is a lack of clarity concerning conditional licenses.

We believe the proposal, if adopted, will: (1) create a dangerous patchwork of state laws ill-suited to a technology without borders; (2) harm anonymous speech; (3) undermine innovation in digital currency businesses; (4) harm innovation in blockchain technologies; and (5) create needless cybersecurity risks.

I. STATE REGULATION IS INAPPROPRIATE

The NYDFS should not adopt this proposal because states should simply not be in the business of adopting state-specific rules on digital currencies.

³ Matt Mullenweng, *On WordPress.com and Bitcoin*, Feb. 24, 2015, <http://ma.tt/2015/02/on-wordpress-com-and-bitcoin/>

First, a New York law will impact businesses and consumers across the nation, who do not have the slightest nexus to (or political rights in) New York. As everyone understands, this state proposal will have a national impact – all Internet businesses have some users in New York State, and that is all it takes to fall under the purview of the proposed regulations.

Second, other states will likely follow suit by adopting their own regulations, and conflicts among state laws will impose redundant expenses and potentially competing and contradictory mandates. To begin, the requirement to pay a licensing fee and submit a licensing application in multiple states would require startups that hope to use bitcoin to incur onerous legal fees and filing fees. Despite efforts by the Conference of State Bank Supervisors to adopt nationwide standards based on the Nationwide Multi-State Licensing System and Registry, it remains unclear whether these efforts will succeed in reducing duplication or conflicts.⁴

Third, the state impacts on distributed ledgers would likely violate the Constitution's dormant commerce clause. Distributed ledgers rely entirely on the Internet, and federal regulation, not a state patchwork, generally governs Internet activities. The FCC preempts state Internet access regulation,⁵ long-standing Congressional action bans Internet-specific state taxes,⁶ and court decisions relying on the dormant commerce clause invalidate state Internet laws for their extraterritorial effect.⁷ Both policy and the dormant commerce clause counsel against encouraging fractured state-level laws for bitcoin.

Fourth, beyond the dormant commerce clause, as a matter of policy, new technologies may warrant federal frameworks for previously state-level enforcement. The state seems to assume that because money transmission laws have been historically enacted at the state level, the state should also adopt rules that govern digital currencies, too. Our experience with the Internet suggests the opposite—that new technologies benefit from a uniform federal regulatory framework in lieu of a historically state-level law. For example, while state laws historically governed libel and slander before the Internet, the federal government imposed new federal libel policies.

⁴ Testimony of David J. Cotney, *On "Present and Future Impact of Virtual Currency,"* US Senate, Nov. 19, 2013, <http://www.csbs.org/legislative/testimony/Documents/TestimonyofDavidCotneyVirtualCurrencyTestimonySenateBankingNov2013.pdf>

⁵ *Preserving the Open Internet*, 25 FCC Rcd 17905, 17970, n.374 (2010), affirmed in part, vacated in part, in *Verizon v. FCC*, 740 F.3d 623 (D.C. Cir. 2014).

⁶ Grant Gross, *Internet Tax Moratorium Extended Again*, PC WORLD, Dec. 15, 2014, <http://www.pcworld.com/article/2859872/internet-tax-moratorium-extended-in-us-govt-spending-package.html>

⁷ *Center For Democracy & Technology v. Pappert*, 337 F.Supp.2d 606, 662 (E.D. Pa. 2004).

Congress adopted Section 230 of the Communications Decency Act of 1996, which forbids states from imposing liability on ISPs that merely transmit libelous speech.⁸ This federal policy is among the most celebrated of Internet laws for ensuring that fifty state laws do not constrain Internet intermediaries. This history suggests that, if digital currencies are to be regulated, then New York would be wise to leave this area of law for regulation at the federal level, which is better suited for promoting innovation and liberty online, even if state regulation of previous technologies was the norm.

II. THE NYDFS PROPOSAL HARMS ANONYMOUS SPEECH

At Automattic, we see that many of our users choose to publish their sites anonymously. This is especially true for users in countries lacking freedom of expression: if their identity were known, their words would put them in danger. An advantage of bitcoin is that it allows these anonymous publishers some great ability to protect themselves from discovery. Relatively more identifiable forms of payment, including credit card payments, may be a matter of life and death for these brave writers. This proposal would require anonymous publishers to risk revealing their identities merely to pay a small amount for premium features, such as a custom domain name for their website. Moreover, the proposed rule's requirement that real names be stored for seven years and available to the NYDFS essentially creates a hit list for some of the totalitarian nations in which our anonymous users reside.

III. THE PROPOSAL HARMS INNOVATION IN DIGITAL CURRENCY GENERALLY AND SPECIFICALLY IN MICROPAYMENTS

By increasing the costs of using distributed ledgers—through licensing, record-keeping, and state-level regulatory legal compliance—the proposal will reduce innovation in the digital currency market, including undermining potential benefits to media outlets and bloggers using distributed ledgers for micropayments.

First, raising the cost of innovation will lead to less innovation in this market—or at best push this innovation to friendlier jurisdictions abroad, such as in the UK where the government

⁸ Communications Decency Act of 1996, 47 U.S.C. § 230 (2006); Marvin Ammori, *The "New" New York Times*, 127 HARV. L. REV. 2259, 2260 (2014).

recently announced a framework that is far more friendly.⁹ Innovation in the face of uncertainty requires low costs of innovation and a high number of potential entrants. Despite venture capitalists and corporate executives trying their best, no one can predict which innovations will succeed. Research suggests that centralized planning, licensing, and investment by established players does not lead to incremental or disruptive innovation nearly as well as decentralized innovation by independent entities and people with varying skills and backgrounds, and by outsiders, immigrants, and upstarts.¹⁰ Based on this research, keeping the costs of innovation low and removing all barriers would lead to greater innovation and—since innovation is a key driver of economic growth—an expanding economy.

At Automattic, we strongly believe in an economy with very low costs imposed on innovators of all stripes—large corporations, startups, small businesses, open source projects, nonprofits, and individuals. That is why we contribute to the WordPress community, which supports an open source software platform that serves as a foundation for millions of websites and applications built on top of it, none of which many of the project’s contributors could have imagined or planned.

Bitcoin too is an open source innovation that can be the basis for unforeseeable entrepreneurship and public service. We can imagine some general use cases: providing banking for underserved communities,¹¹ facilitating remittances to countries around the world,¹² and helping nonprofits collect small donations. The core innovation of the distributed ledger may impact a wide range of industries across the economy and around the world. We are barely at the dawn of what distributed ledgers can enable. With the history of the Internet itself as a guide, the best course of action for regulators at all levels of government is to take a hands-off approach for now for this new software innovation. The costs of regulation imposed on digital currency businesses relying on open source innovations like bitcoin can only serve to lessen the possibilities

⁹ The new UK digital currency framework does not require a license for digital currency companies, but instead will create a voluntary, opt-in consumer protection standard regime, implement AML laws only for exchanges, and devote an annual budget of \$15M to pursue digital currency research. *See* <https://www.gov.uk/government/consultations/digital-currencies-call-for-information>

¹⁰ BARBARA VAN SCHEWICK, INTERNET ARCHITECTURE AND INNOVATION (MIT 2010).

¹¹ According to the FDIC, there are 93 million Americans that are un- or underbanked. *See* <https://www.fdic.gov/news/news/press/2014/pr14091.html>

¹² According to the World Bank, the average fee on remittances is 8%, but charges can be three times as much. *See* https://remittanceprices.worldbank.org/sites/default/files/rpw_report_january_2015.pdf

for groundbreaking new developments in payments, financial services, and decentralized technologies of all kinds.

Second, the proposal may harm one specific innovation that we can already imagine: micropayments for bloggers, publishers, and media outlets. Micropayments generally are payments of less than a dollar and may include things like songs, in-app or in-game purchases, tipping or donation services, and other emerging business models. As news and commentary have moved from print to digital, and as outlets therefore face more local and international competition for advertising dollars, some media companies have experimented with micro-transactions. Notably, the Chicago Sun-Times has run experiments to determine that readers may contribute a quarter to access its site on a day.¹³ Other media outlets—and bloggers—can also rely on micropayments to supplement or replace advertising income. Readers could in theory “tip” or “contribute” to authors, and small amounts from a large number of users could turn into a sustainable revenue stream, whether it is a supplemental or primary stream.

These micropayments are only possible where transaction costs are nearly nonexistent—a possibility with digital currency, but currently not practical on legacy payments systems. Credit card transactions cost between 2% and 5%, plus minimum fees of at least 30 cents, regardless of the size of transaction. As one analyst noted, “let’s say I wanted to pay five cents to read an article – with PayPal or Visa, payment processing might cost 50 cents,” meaning the transaction cost would be ten times the actual payment.¹⁴ Bitcoin and other digital currencies, by contrast, have much lower fees, and bitcoin businesses have created products with no fees.¹⁵ With fees of less than a cent, digital currency can potentially make possible a micropayment business model that would have a transformative impact in media and blogging.

One solution is to create a safe harbor for micropayment platforms along the lines of the key safe harbors that enabled the Internet to flourish, DMCA §512 and CDA §230. A safe harbor

¹³ Pete Rizzo, *Chicago Sun-Times Bitcoin Paywall Shows 25 Cents is Sweet Spot*, COINDESK, Feb. 6, 2014, <http://www.coindesk.com/chicago-sun-times-bitcoin-paywall-25-cents/>; Michael Carney, *Why the Chicago Sun-Times Bitcoin Experiment is More than a Desperate Attempt to Look Cool*, PANDO DAILY, Jan. 14, 2014, <http://pando.com/2014/01/14/why-the-chicago-sun-times-bitcoin-paywall-experiment-is-more-than-a-desperate-attempt-to-look-cool/>

¹⁴ Jerry Brito, *A Bitcoin for Your Thoughts*, MARK NEWS, July 14, 2011, <http://pioneers.themarknews.com/articles/6018-a-bitcoin-for-your-thoughts/#.VPLDpLDF-free> speech

¹⁵ *You Can Now Send Micro-transactions with Zero Fees*, COINBASE BLOG, Aug. 5, 2013, <http://blog.coinbase.com/post/57483182558/you-can-now-send-micro-transactions-with-zero-fees>

would enable the transmission of smaller amounts (similar to those amounts allowed for prepaid cards) in exchange for following standards in security best practices and consumer protection. This approach would not require a license, but would instead promote good behavior among innovators without quelling the development of new technology. One such proposal is being circulated in letter form and is worth considering.¹⁶

IV. THE PROPOSAL HARMS BLOCKCHAIN INNOVATION

The proposal likely harms innovation in distributed ledger technologies beyond those used as currency substitutes. DFS's proposal requiring a license for "controlling, administering, or issuing a virtual currency" would negatively affect much of the second wave of bitcoin innovation. For example, private companies in the future may well issue their stock on a new type of blockchain called a sidechain, one that is backed by the bitcoin currency itself. If so, the proposal could require these companies to obtain a license. Many other open source innovations that use tokens for, say, decentralized file storage or a platform to create new applications, would also be required to obtain a license. This licensing provision may stamp out the next generation of bitcoin technology at worst, or at best ensure that new protocols are designed with New York users excluded from any implementation.

V. THE PROPOSAL HARMS CYBERSECURITY

The proposal, if adopted, would impose unnecessary and harmful obligations that would diminish rather than enhance cybersecurity. The Department could create a nightmare scenario where transmitters will take on the burdens of gathering and filing annual reports under Section 200.16(d) that would expose multiple companies' security procedures to anyone who manages to hack the Department or fool a Department employee. The Department will have a bullseye on its systems. It should remove the entire set of provisions under the principle of "first, do no harm."

The Department's proposal has many fatal flaws, including being onerous, redundant, and counterproductive.

¹⁶ Elizabeth Stark, *The BitLicense Needs a Safe Harbor*, Mar. 24, 2015, <http://bitsafeharbor.org>

First, the definition of cybersecurity event is astonishingly broad and therefore onerous. The definition includes “any ... *attempt*, successful or unsuccessful, to gain unauthorized access” to “electronic systems” or “information stored on such systems.”¹⁷ This definition clearly does not understand the state of play: most players, especially large ones or those in the financial sector, are under attack most of the time. A Congressional report in 2013 revealed that, for example, utilities are under “constant” attack and one provider estimated 10,000 attempted intrusions a month.¹⁸ According to this Department’s own report on cybersecurity in the banking sector, “Most institutions irrespective of size experienced intrusions or attempted intrusions into their IT systems over the past three years.”¹⁹ Therefore, since merely an “attempt” would trigger notification (or another regulatory burden), this definition is completely unworkable. The Department should look to definitions in leading state data breach notification statutes or proposed federal legislation, which generally reference a risk-based trigger such as the reasonable belief that a breach “has caused or will cause identity theft or other actual financial harm” to residents.²⁰ Indeed, the Department’s own report on cybersecurity in the banking sector noted merely that banks generally reported a “breach”—not an attempt—and seemed to understand (when discussing banks) why that makes sense.²¹ The same principle of considering breaches (not attempts) applies here, as reflected in leading state data breach notification laws.

Second, New York already has a state data breach notification law and one small subset of emerging companies should not be subject to higher and different standards than banks, energy and electric companies, and major retailers. The New York law defines breach narrowly based on access to specifically defined “personal information” and “private information,” as well as whether the information is “reasonably believed to have been acquired.”²² This state law is general—not targeting a new sector—and its requirements are more appropriate to the harms. Moreover, when the Department deals with the traditional banking and insurance sector, the Department relies on “surveys,” conversations, and encouragement, recognizing that “cyber security does not have a

¹⁷ Section 200.2(b).

¹⁸ Ed Markey & Henry Waxman, “*Electric Grid Vulnerability: Industry Responses Reveal Security Gaps*,” May 21, 2013, <http://democrats.energycommerce.house.gov/sites/default/files/documents/Report-Electric-Grid-Vulnerability-2013-5-21.pdf>.

¹⁹ NYDFS, *Report on Cyber Security in the Banking Sector*, May 2014, at 9.

²⁰ See, e.g., S.1193 - Data Security and Breach Notification Act of 2013.

²¹ NYDFS, *Report on Cyber Security in the Banking Sector*, May 2014, at 9.

²² N.Y. GBS. LAW § 899-aa: NY Code - Section 899-AA.

‘one-size fits-all’ solution.”²³ The Department also found that a large number of smaller institutions had less well-developed cybersecurity programs than larger institutions, but did not impose additional or needless obligations for that reason. The Department has not justified singling out one particular sector even though New York law—and the Department’s own actions for other businesses—are much different and more appropriate.

Moreover, there is no demonstrated need for a specific digital currency cybersecurity law. If the Department seeks to adopt a general cybersecurity law for the entire banking or financial sector, it should not impose new rules first for a tiny subset of new entrants into the industry and then extend them to established players. Better governance requires taking specific comment on rules for the entire industry from the entire industry—and adapting the proposal based on those informed comments. The Department would either have an incomplete record for a broader rule if adopted now or would adopt a different and perhaps more sensible one only for non-bitcoin players if it were to incorporate sensible future comments in an industry-wide rulemaking. Even if the Department eventually transitioned these requirements on digital currency innovators over to a broader industry-wide rule, as they have stated an intention to do,²⁴ there is no reason to impose differing, likely more onerous rules today in the interim—an interim that may last months or years.

Third, the proposal requires licensees to file cybersecurity plans, but these filings would harm, not strengthen, cybersecurity. Transmitters must file cybersecurity policies with the Department,²⁵ and these policies must include thirteen areas including “access controls,” “systems and network security,” “physical security and environmental controls,” and “capacity and performance planning.”²⁶ In addition, the proposal requires the Chief Security Officer (a position required by the proposal) to file annual reports identifying “relevant cyber risks” and “proposing steps for the redress of any inadequacies identified therein.”²⁷ The requirement to file these policies and reports would provide a roadmap to potential intruders. The first stop in an intruder’s road would be the one pot of honey known to hold all these policies: the Department itself. This requirement imposes system-wide cybersecurity risk by concentrating all these policies and reports

²³ NYDFS, *Report on Cyber Security in the Banking Sector*, May 2014, at 11. See also NYDFS, *Report on Cyber Security in the Insurance Sector*, Feb. 2015, at 2.

²⁴ Benjamin Lawskey, *Keynote at Money 2020*, Nov. 2, 2014, <https://www.youtube.com/watch?v=d6csV7OkPbA>.

²⁵ Section 200.4(a)(9).

²⁶ Section 200.16(b).

²⁷ Section 200.16(a).

in the Department's hands. It is not at all clear that the Department has cybersecurity procedures in place to handle that enormous risk.

Fourth, the proposal would impose unrealistic requirements. It would require an "effective" cybersecurity program that "shall be designed to perform" five functions including to "detect systems intrusions, data breaches, unauthorized access to systems or information, malware, and other Cyber Security Events."²⁸ No system can be designed to detect all intrusions and breaches, which is why more sensible legislation turns on "reasonable belief" of such intrusions. Similarly, the Department does not define "effective," and no program is 100% effective against every attempted intrusion.

Fifth, the rules require regulated companies to "respond to detected Cyber Security Events to mitigate any negative effects," but should qualify that often companies cannot respond because the attack may be over by the time it is discovered and that companies certainly cannot mitigate "any" negative effects. That standard is unreasonable.

Finally, many of the cybersecurity requirements may become obsolete, in light of the dynamic pace of change in this industry, and blockchain and encryption technology have the capacity to pose superior solutions. For example, this revised draft of the proposal wisely removed the requirement to enclose "hardware in locked cages" as that is no longer a best practice. Using a technology like the blockchain to enable distributed, personalized data storage encrypted on a user's device may entirely change the concept of a data breach. This dynamism is one more reason the Department should follow the usual practices of the state data breach notification law and its approaches in the banking and insurance sector, rather than imposing new mandates.

For all of these reasons—the inappropriate role of state regulation, the harm to anonymous speech, innovation, and cybersecurity—the Department should not adopt this proposal.

Best Regards,

Paul Sieminski
General Counsel, Automattic Inc.

Marvin Ammori
Principal, Ammori Group
Counsel to Automattic

²⁸ Section 200.16(a)(3).