

## **ATTACHMENT A: STATEMENT OF FACTS AND VIOLATIONS**

### **I. INTRODUCTION AND BACKGROUND**

1. Ripple Labs Inc. (“Ripple Labs”) is a corporation registered in Delaware and headquartered in San Francisco, California. NewCoin, Inc. and OpenCoin, Inc. (“OpenCoin”) are the predecessors of Ripple Labs.
2. Ripple Labs facilitated transfers of virtual currency and provided virtual currency exchange transaction services.
3. The currency of the Ripple network, known as “XRP,” was pre-mined. In other words, unlike some other virtual currencies, XRP was fully generated prior to its distribution. As of 2015, XRP is the second-largest cryptocurrency by market capitalization, after Bitcoin.
4. XRP Fund II, LLC, a wholly-owned subsidiary of Ripple Labs, was incorporated in South Carolina on July 1, 2013. On July 2, 2014, XRP Fund II changed its name to XRP II, LLC. During a portion of the relevant timeframe, the entity was named XRP Fund II, LLC, but it will be referred to as XRP II throughout this document.

### **II. LEGAL FRAMEWORK**

5. The U.S. Attorney’s Office for the Northern District of California (“U.S. Attorney’s Office”) is a component of the Justice Department. The Financial Crimes Enforcement Network (“FinCEN”) is a bureau within the Department of Treasury. The Bank Secrecy Act and its implementing regulations require Money Services Businesses (“MSBs”) to register with FinCEN by filing a Registration of Money Services Business (“RMSB”), and renewing the registration every two years. *See* 31 U.S.C. § 5330; 31 C.F.R. § 1022.380. Operation of an MSB without the appropriate registration also violates federal criminal law. *See* 18 U.S.C. § 1960(b)(1)(B). This is a requirement separate and apart from state licensing requirements, if any, that may be required by law.
6. On March 18, 2013, FinCEN released guidance clarifying the applicability of regulations implementing the Bank Secrecy Act, and the requirement for certain participants in the virtual currency arena to register as MSBs under federal law. *See* FIN-2013-G0001, Application of FinCEN’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (Mar. 18, 2013) (the “Guidance”). Among other things, the Guidance defines two categories of participants in the virtual

currency ecosystem: “exchangers” and “administrators.” The Guidance states that exchangers and administrators of virtual currencies are money transmitters (a type of MSB) under FinCEN’s regulations, and therefore are required to register with FinCEN as money service businesses.

7. Specifically, the Guidance defines an exchanger as a person or entity “engaged as a business in the exchange of virtual currency for real currency, funds, or other virtual currency.” The Guidance also defines an administrator of virtual currency as a person or entity “engaged as a business in issuing (putting into circulation) a virtual currency, and who has the authority to redeem (to withdraw from circulation) such virtual currency.”
8. Both exchangers and administrators are MSBs that must register with FinCEN unless they fall within an exemption. And regardless of whether they have registered as required, MSBs are subject to certain additional requirements under the Bank Secrecy Act and its implementing regulations.
9. The Bank Secrecy Act and its implementing regulations require MSBs to develop, implement, and maintain an effective written anti-money laundering (“AML”) program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities. *See* 31 U.S.C. §§ 5318(a)(2) and 5318(h); 31 C.F.R. § 1022.210.
10. Under the Bank Secrecy Act, an MSB is required to implement an AML program that, at a minimum: (a) incorporates policies, procedures and internal controls reasonably designed to assure ongoing compliance; (b) designates an individual responsible for assuring day to day compliance with the program and Bank Secrecy Act requirements; (c) provides training for appropriate personnel including training in the detection of suspicious transactions; and (d) provides for independent review to monitor and maintain an adequate program. 31 C.F.R. §§ 1022.210(d).
11. Further, an MSB must report transactions that the MSB “knows, suspects, or has reason to suspect” are suspicious, if the transaction is conducted or attempted by, at, or through the MSB, and the transaction involves or aggregates to at least \$2,000.00 in funds or other assets. 31 C.F.R. § 1022.320(a)(2). A transaction is “suspicious” if the transaction: (a) involves funds derived from illegal activity; (b) is intended or conducted in order to hide or disguise funds or assets derived from illegal activity, or to disguise the ownership, nature, source, location, or control of funds or assets derived from illegal activity; (c) is designed, whether through structuring or other means, to evade any requirement in the Bank Secrecy Act or its implementing regulations; (d) serves no business or apparent lawful purpose, and the MSB knows of

no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction; or (e) involves use of the MSB to facilitate criminal activity. *Id.*

12. As part of their risk assessment and risk mitigation plans, MSBs are required to implement Know-Your-Customer/Know-Your-Counterparty procedures. Such procedures allow the MSB to assess the risk involved in providing account-based or transactional services to customers based on their identity and profile, and to comply with their AML Program requirements regarding foreign agents or foreign counterparties. *See* FinCEN Interpretive Release 2004-1, Anti-Money Laundering Program Requirements for Money Service Businesses With Respect to Foreign Agents or Foreign Counterparties, 69 Fed. Reg. 74,439 (Dec. 14, 2004).
13. Financial institutions, including MSBs, are also subject to the Funds Transfer Rule, 31 C.F.R. § 1010.410(e), which provides that (subject to certain exceptions) for individual transactions of \$3,000.00 or above, the transmitting financial institution must obtain, verify, and keep key information (set forth in the regulation) from the transmitting party (the transmitter). If acting as an intermediary financial institution, it must obtain and keep key information (the transmittal order received) from the transmitter's financial institution. And, if acting as the financial institution for the recipient of the funds, the financial institution must obtain, verify, and keep key information (also set forth in the regulation) from the recipient. The same financial institution may be acting as both transmitter's and recipient's financial institution.
14. Similarly, financial institutions, including MSBs, are subject to the Funds Travel Rule, 31 C.F.R. § 1010.410(f), which provides that (subject to certain exceptions) for individual transactions of \$3,000.00 or more, the transmitter's financial institution must pass on key information from the transmitter and the transaction to any intermediary financial institution; if acting as the intermediary financial institution, it must pass on this information to the recipient's financial institution. And, if acting as the recipient's financial institution, it must receive, evaluate, and store this information received from the intermediary or the transmitter's financial institution.
15. The FinCEN registration requirement and other requirements of the Bank Secrecy Act are independent obligations. An MSB's failure to register with FinCEN does not relieve an MSB of its obligations under the Bank Secrecy Act and implementing regulations. Nor does an MSB's registration with FinCEN mean that the MSB has fulfilled all of its requirements under the Bank Secrecy Act and regulations. In other words, an MSB might have complied with the Bank Secrecy Act and implementing regulations, but failed to register as an MSB with FinCEN. Likewise, an entity might

have registered as an MSB with FinCEN, but not have complied with the Bank Secrecy Act and implementing regulations.

### III. VIOLATIONS

#### A. Ripple Labs's Operation as a Money Services Business in March-April 2013

16. Ripple Labs has previously described itself in federal court filings and in a sworn affidavit as “a currency *exchange service* providing on-line, real-time currency trading and cash management . . . . Ripple facilitates the transfers of electronic cash equivalents and provides virtual currency exchange transaction services for transferrable electronic cash equivalent units having a specified cash value.” *See Ripple Labs, Inc. v. Lacore Enterprises, LLC*, Motion for Preliminary Injunction, 13-cv-5974-RS/KAW (N.D. Cal. 2013) (emphasis added).
17. From at least March 6, 2013, through April 29, 2013, Ripple Labs sold convertible virtual currency known as “XRP.”
18. Ripple Labs was not registered with FinCEN as an MSB while engaging in these sales.
19. As described in Paragraphs 6 and 7 above, on March 18, 2013, FinCEN released guidance that clarified the applicability of existing regulations to virtual currency exchangers and administrators. Among other things, this Guidance expressly noted that such exchangers and administrators constituted “money transmitters” under the regulations, and therefore must register as MSBs.
20. Notwithstanding the Guidance, and after that Guidance was issued, Ripple Labs continued to engage in transactions whereby it sold Ripple currency (XRP) for fiat currency (*i.e.*, currency declared by a government to be legal tender) even though it was not registered with FinCEN as an MSB. Throughout the month of April 2013, Ripple Labs effectuated multiple sales of XRP currency totaling over approximately \$1.3 million U.S. dollars.
21. During the time frame that it was engaged in these sales and operated as a money transmitter, Ripple Labs failed to establish and maintain an appropriate anti-money laundering program. Ripple failed to have adequate policies, procedures, and internal controls to ensure compliance with the Bank Secrecy Act and its implementing regulations. Moreover, Ripple Labs failed to designate a compliance officer to assure compliance with the Bank Secrecy Act, had no anti-money laundering training in place, and failed to have any independent review of its practices and procedures.

**B. XRP II's Program and Reporting Violations**

22. On July 1, 2013, Ripple Labs incorporated a subsidiary, XRP Fund II, LLC ("XRP Fund II"), now known as XRP II, LLC, in South Carolina. XRP II was created to engage in the sale and transfer of the convertible virtual currency, XRP, to various third parties on a wholesale basis. XRP II sold XRP currency in exchange for fiat currency in much the same way that Ripple Labs had previously done from March through April 2013. In other words, XRP II replaced Ripple Labs as a seller of XRP.
23. By on or about August 4, 2013, XRP II was engaged in the sale of XRP currency to third-party entities.
24. On September 4, 2013, XRP II registered with FinCEN as an MSB.
25. As of the date XRP II engaged in sales of virtual currency to third parties in exchange for value, XRP II became subject to certain requirements under the Bank Secrecy Act and its implementing regulations, as described in Paragraphs 5 through 15 above. XRP II was required to have an effective written AML program, to implement that program, and to have an anti-money laundering compliance officer.
26. Notwithstanding these requirements, despite engaging in numerous sales of virtual currency to third parties, XRP II failed to have an effective, written AML program. For example:
  - a) It was not until September 26, 2013, that XRP II developed a written AML program. Prior to that time, XRP II had no written AML program;
  - b) It was not until late January 2014 that XRP II hired an AML compliance officer, some six months after it began to engage in sales of virtual currency to third parties;
  - c) XRP II had inadequate internal controls reasonably designed to ensure compliance with the Bank Secrecy Act;
  - d) XRP II failed to conduct an AML risk assessment until March 2014;
  - e) XRP II did not conduct training on its AML program until nearly a year after beginning to engage in sales of virtual currency, by which time Ripple Labs was aware of a federal criminal investigation; and

- f) XRP II did not conduct an independent review of its AML program until nearly a year after it began to engage in sales of virtual currency, by which time Ripple Labs was aware of a federal criminal investigation.
27. Further, from the date XRP II began engaging in sales of virtual currency to third parties, XRP II was required to report transactions that it knew, suspected, or had reason to suspect were suspicious and where the transactions or attempted transactions involved or aggregated to at least \$2,000.00 in funds or other assets. *See* 31 C.F.R. § 1022.320(a)(2).
28. In addition to XRP II's lack of an effective AML program, XRP II also engaged in a series of transactions for which it either failed to file, or untimely filed, suspicious activity reports. For example:
- a) On September 30, 2013, XRP II negotiated an approximately \$250,000.00 transaction by email for a sale of XRP virtual currency with a third-party individual. XRP II provided that individual with a "know your customer" ("KYC") form and asked that it be returned along with appropriate identification in order to move forward with the transaction. The individual replied that another source would provide the XRP virtual currency and did not "require anywhere near as much paperwork" and essentially threatened to go elsewhere. Within hours, XRP II agreed by email to dispense with its KYC requirement and move forward with the transaction. Open source information indicates that this individual, an investor in Ripple Labs, has a prior three-count federal felony conviction for dealing in, mailing, and storing explosive devices and had been sentenced to prison, *see United States v. Roger Ver*, CR 1-20127-JF (N.D. Cal. 2002);
  - b) In November 2013, XRP II rejected an approximately \$32,000.00 transaction because it doubted the legitimacy of the overseas customer's source of funds. XRP II failed to file a suspicious activity report for this transaction; and
  - c) In January 2014, a Malaysian-based customer sought to purchase XRP from XRP II, indicating that he wanted to use a personal bank account for a business purpose. Because of these concerns, XRP II declined the transaction but again failed to file a suspicious activity report for the transaction.