



## U.S. Department of Justice

*United States Attorney  
Northern District of California*

---

### SETTLEMENT AGREEMENT

On the understandings specified below, the United States Attorney's Office in the Northern District of California (the "Government") will not criminally prosecute Ripple Labs Inc., a Delaware Corporation headquartered in San Francisco, California, and any and all subsidiaries of Ripple Labs Inc., (collectively "Ripple Labs" or the "Company") for any of the conduct described in the Statement of Facts, attached as Attachment A. The Government enters into this Settlement Agreement ("Agreement") based on the individual facts and circumstances presented by this case and the Company. Among the factors considered were the following: (a) the Company's extensive cooperation with the Government; (b) the Company has committed to continue to enhance its pre-existing Anti-Money Laundering program and training and internal controls as set forth in Attachment B; (c) the Company has agreed to migrate a component of its business as set forth in Attachment B; and (d) the Company has agreed to continue to cooperate with the Government in any known, ongoing investigation of the conduct of the Company and its officers, directors, employees, agents, and consultants relating to violations of the Bank Secrecy Act. The Company enters into this Agreement under authority granted by its Board of Directors in the form of a Board Resolution, a copy of which is attached as Attachment C.

The Company admits, accepts, and acknowledges that it is responsible under United States law for the acts of its officers, directors, employees, and agents as set forth in the Statement of Facts attached hereto as Attachment A and incorporated by reference into this Agreement, and that the facts described in Attachment A are true and accurate. The Company expressly agrees that it shall not, through present or future attorneys, officers, directors, employees, agents or any other person authorized to speak for the Company make any public statement, in litigation or otherwise, contradicting the acceptance of responsibility by the Company set forth above or the facts described in the Statement of Facts attached hereto as Attachment A.

The Company's obligations under this Agreement shall have a term of three (3) years from the date that this Agreement is executed. However, the Company shall continue to cooperate fully with the Government in any and all matters relating to Bank Secrecy Act violations, subject to applicable law and regulations, until the date upon which all investigations and prosecutions arising out of the conduct described in this Agreement are concluded, whether or not those investigations are concluded within the term specified herein. The Company agrees that its cooperation pursuant to this paragraph shall include, but is not limited to, the following:

- a) The Company shall truthfully disclose, consistent with applicable law and regulations including data protection and privacy laws, all information not protected by a valid claim of privilege or work product with respect to its activities, those of its parent company and affiliates, and those of its present and former directors, officers,

employees, agents, and consultants concerning all matters relating to violations of the Bank Secrecy Act about which the Company has any knowledge or about which the Government may inquire. This obligation of truthful disclosure includes the obligation of the Company to provide to the Government, upon request, any document, record or other tangible evidence relating to such violations of the Bank Secrecy Act about which the Government may inquire of the Company.

- b) Upon request of the Government, with respect to any issue relevant to its investigation of violations of the Bank Secrecy Act in connection with the operations of the Company, or any of its present or former subsidiaries or affiliates, the Company shall designate knowledgeable employees, agents or attorneys to provide to the Government the information and materials described in (a) above on behalf of the Company. It is further understood that the Company must at all times provide complete, truthful, and accurate information.
- c) With respect to any issue relevant to the Government's investigation of violations of the Bank Secrecy Act in connection with the operations of the Company, its parent company, or any of its present or former subsidiaries or affiliates, the Company shall ensure that the Government is given access to all current and, to the extent possible, former directors, officers, employees, agents, and consultants of the Company for interviews and testimony in the United States. This obligation includes, but is not limited to, sworn testimony before a federal grand jury or in federal trials, as well as interviews with federal law enforcement and regulatory authorities. Cooperation under this Paragraph shall include identification of witnesses who, to the knowledge of the Company, may have material information regarding the matters under investigation.
- d) With respect to any information, testimony, documents, records or other tangible evidence provided to the Government pursuant to this Agreement, the Company consents to any and all disclosures, subject to applicable law and regulations, to other governmental authorities, including United States authorities of such materials as the Government, in its sole discretion, shall deem appropriate.

The Company represents that it has implemented and will continue to implement a compliance program as described in Attachment B, designed to prevent and detect violations of the Bank Secrecy Act throughout its operations, including those of its affiliates, agents, and joint ventures.

The Company agrees to pay forfeiture in the amount of \$450,000.00 in the form of a cashier check payable to the United States Treasury Department within thirty (30) business days of signing of this Settlement Agreement by sending the cashier check to the United States Attorney's Office, Attn: AUSA Kathryn Haun and AUSA Arvon J. Perteet, 450 Golden Gate Avenue, 11<sup>th</sup> floor, San Francisco, CA, 94102. The Company acknowledges that no United States tax deduction may be sought in connection with the payment of any part of this \$450,000.00 forfeiture.

The Government agrees, except as provided herein, that it will not bring any criminal or civil case against the Company relating to any of the conduct described in the Statement of Facts, attached as Attachment A hereto. The Government, however, may use any information related to the conduct described in the attached Statement of Facts against the Company: (a) in a prosecution for perjury or obstruction of justice; (b) in a prosecution for making a false statement; (c) in a prosecution or other proceeding relating to any crime of violence; or (d) in a prosecution or other proceeding relating to a violation of any provision of Title 26 of the United States Code; provided that any such prosecution or other proceeding does not relate to any potentially obstructive conduct disclosed by the Company to the Government prior to the signing of this Agreement. This Paragraph does not provide any protection against prosecution for any future conduct by the Company. In addition, this Paragraph does not provide any protection against prosecution of any present or former officer, director, employee, shareholder, agent, consultant, contractor, or subcontractor of the Company for any violations committed by them.

If, during the term of this Agreement, the Government determines, in its sole discretion, that the Company has breached the Agreement by (a) committing any felony under U.S. federal law subsequent to the signing of this Agreement, (b) at any time providing in connection with this Agreement deliberately false, incomplete, or misleading information, (c) failing to cooperate as set forth in this Agreement, (d) committing acts that, had they occurred within the jurisdictional reach of the Bank Secrecy Act, would be a violation of the Bank Secrecy Act, or (e) otherwise failing specifically to perform or to fulfill completely each and every one of the Company's obligations under the Agreement, the Company shall thereafter be subject to prosecution for any federal criminal violation of which the Government has knowledge. Any such prosecution may be premised on information provided by the Company. Any such prosecution that is not time-barred by the applicable statute of limitations on the date of the signing of this Agreement may be commenced against the Company notwithstanding the expiration of the statute of limitations between the signing of this Agreement and the expiration of the term of this Agreement plus one year. Thus, by signing this Agreement, the Company agrees that the statute of limitations with respect to any such prosecution that is not time-barred on the date of the signing of this Agreement shall be tolled for the term of this Agreement plus one year.

In the event that the Government determines that the Company has breached this Agreement, the Government agrees to provide the Company with written notice of such breach prior to instituting any prosecution resulting from such breach. Within thirty (30) days of receipt of such notice, the Company shall have the opportunity to respond to the Government in writing to explain the nature and circumstances of such breach, as well as the actions the Company has taken to address and remediate the situation, which explanation the Government shall consider in determining whether to institute a prosecution.

In the event that the Government determines that the Company has breached this Agreement: (a) all statements made by or on behalf of the Company to the Government or to the Court, including the attached Statement of Facts, and any testimony given by the Company before a grand jury, a court, or any tribunal, or at any legislative hearings, whether prior or subsequent to this Agreement, and any leads derived from such statements or testimony, shall be admissible in evidence in any and all criminal proceedings brought by the Government against the Company; and (b) the Company shall not assert any claim under the United States

Constitution, Rule 11(f) of the Federal Rules of Criminal Procedure, Rule 410 of the Federal Rules of Evidence, or any other federal rule that statements made by or on behalf of the Company prior or subsequent to this Agreement, or any leads derived therefrom, should be suppressed or are otherwise inadmissible. The decision whether conduct or statements of any current director or employee, or any person acting on behalf of, or at the direction of, the Company will be imputed to the Company for the purpose of determining whether the Company has violated any provision of this Agreement shall be in the sole discretion of the Government.

This Agreement is binding on the Company and the Government but specifically does not bind any other federal agencies, or any state, local or foreign law enforcement or regulatory agencies, or any other authorities, although the Government will bring the cooperation of the Company and its compliance with its other obligations under this Agreement to the attention of such agencies and authorities if requested to do so by the Company. It is further understood that the Company and the Government may disclose this Agreement to the public.

*(continued on page 5)*

This Agreement sets forth all the terms of the agreement between the Company and the Government. No amendments, modifications or additions to this Agreement shall be valid unless they are in writing and signed by the Government, the attorneys for the Company, and a duly authorized representative of the Company.

MELINDA HAAG  
United States Attorney

DATE: \_\_\_\_\_

BY: \_\_\_\_\_  
KATHRYN HAUN  
Assistant United States Attorney

DATE: \_\_\_\_\_

BY: \_\_\_\_\_  
ARVON J. PERTEET  
Assistant United States Attorney

AGREED AND CONSENTED TO:

DATE: \_\_\_\_\_

BY: \_\_\_\_\_  
NORMAN REED  
General Counsel  
Ripple Labs Inc.

APPROVED BY:

DATE: \_\_\_\_\_

BY: \_\_\_\_\_  
GRANT P. FONDO  
Goodwin Procter LLP

DATE: \_\_\_\_\_

BY: \_\_\_\_\_  
MATTHEW L. SCHWARTZ  
Boies, Schiller & Flexner LLP

## ***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.

## ***ATTACHMENT B: REMEDIAL FRAMEWORK***

### 1. Monetary Penalties:

Ripple Labs Inc. and XRP II, LLC (formerly known as XRP Fund II, LLC) agree to forfeit \$450,000.00 to the Office of the United States Attorney for the Northern District of California (“U.S. Attorney’s Office”). Ripple Labs and XRP II further agree to pay a civil money penalty to FinCEN in the amount of \$700,000.00, within 30 days of the date of this agreement. Payment of the forfeiture to the U.S. Attorney’s Office shall be deemed creditable toward FinCEN’s civil money penalty.

### 2. Migration of Ripple Trade/Ripple Wallet to Registered MSB:

Within 30 days of the date of this agreement, Ripple Labs and XRP II will move its service known as Ripple Trade (formerly known as Ripple Wallet, which allows end users to interact with the Ripple protocol to view and manage their XRP and fiat currency balances), and any such functional equivalent, to a money services business that is registered with FinCEN (the “Ripple Trade MSB”).

- a) Any sale or transmission of XRP by Ripple Labs or any of its subsidiaries shall be conducted only through an entity registered with FinCEN;
- b) Users of Ripple Trade (which will include all users registering after the date of this agreement and any existing users who register at the request of Ripple Labs) will be required to submit customer identification information, as required under the rules governing money services businesses, to the Ripple Trade MSB;
- c) Ripple Labs, via the Ripple Trade MSB, will offer incentives, including but not limited to XRP giveaways, for existing Ripple Trade users to transfer a wallet with customer identification information or account (that is, a wallet or account with customer identification information); and
- d) After 180 days of the date of this agreement, Ripple Labs will (1) prevent any existing Ripple Trade user who has not transferred to a wallet or account with customer identification information from accessing the Ripple protocol through the Ripple Trade client, and (2) not otherwise provide any support of any kind to such a user in accessing the Ripple protocol.

3. Maintenance of Registration:  
Ripple Labs and XRP II will maintain, or continue to maintain, XRP II's and the Ripple Trade MSB's registrations with FinCEN, including such re-registrations required by 31 U.S.C. § 5330.
4. Effective AML Program:  
XRP II and the Ripple Trade MSB will implement and maintain, or will continue to maintain, an effective anti-money laundering ("AML") program, risk assessment, and other compliance measures as required by applicable law, including the Bank Secrecy Act and its implementing regulations.
5. AML Compliance Officer:  
XRP II and the Ripple Trade MSB will maintain, or will continue to maintain, an anti-money laundering compliance officer to ensure day-to-day compliance with their obligations under the Bank Secrecy Act and its implementing regulations.
6. Training Program:
  - a) Within 45 days after the date of this agreement, XRP II and the Ripple Trade MSB will create an AML training program for Bank Secrecy Act/AML compliance and will provide a copy of the training program to the U.S. Attorney's Office and FinCEN;
  - b) Within 45 days of the date of this agreement, XRP Fund II and the Ripple Trade MSB will provide training to each of their employees and provide to the U.S. Attorney's Office and FinCEN written evidence of such training, including a certification of such training, the name of each employee who attended such training, and the dates of such training.
7. External audit:  
Within 60 days, XRP II and the Ripple Trade MSB will secure and retain an independent, external, and qualified party or entity (the "Third-Party Reviewer"), not subject to any conflict of interest, and subject to FinCEN's and the U.S. Attorney's Office's determination of non-objection, to examine their Bank Secrecy Act compliance programs and evaluate whether the programs are reasonably designed to ensure and monitor compliance with the requirements of the Bank Secrecy Act and the FinCEN rules applicable to money services businesses. Three reviews will occur: the first will commence within one year of this agreement; the second will occur in 2018; and the third will occur in 2020. Each review will cover the previous two

years, with no less than six months' worth of transactional analysis of those transactions in which XRP II and the Ripple Trade MSB was a party or served as an exchanger. The Third-Party Reviewer will prepare a written report for each company's audit committee and the board of directors, setting forth its findings, and will transmit the report and all draft reports to the U.S. Attorney's Office and FinCEN simultaneously with any transmission to XRP II, the Ripple Trade MSB, or their agents. To the extent that the report identifies any material deficiencies in XRP II's or the Ripple Trade MSB's programs and procedures, XRP II and the Ripple Trade MSB shall address and rectify the deficiencies as soon as is reasonably practicable.

8. Enhancements to Ripple Protocol:

Within 60 days, Ripple Labs, XRP II, and the Ripple Trade MSB will improve, and upon request provide any information requested by FinCEN or the U.S. Attorney's Office as to the use and improvement of, existing analytical tools applicable to the Ripple protocol, including: (1) reporting regarding any counterparty using the Ripple protocol; (2) reporting as to the flow of funds within the Ripple protocol; and (3) reporting regarding the degree of separation.

9. Look-Back for Suspicious Activity:

Within 180 days of the date of this agreement, Ripple Labs and XRP II will conduct a review of all prior transactions and attempted transactions to which Ripple Labs and/or XRP II was a party or served as an exchanger, within the last three years involving or aggregating to at least \$2,000.00 in funds or other assets. For any such transaction for which it is known, suspected, or there is a reason to suspect that the transaction (a) involves funds involved in 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, where 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, Ripple Labs and/or XRP II will file a Suspicious Activity Report within 30 days of such determination.

10. Transaction Monitoring:

Ripple Labs will institute AML programmatic transaction monitoring across the entire Ripple protocol, and will report the results of such monitoring to the U.S. Attorney's Office, FinCEN, and any other law enforcement or regulatory agency

upon request. The monitoring and reporting must include, at a minimum: (a) risk rating of accounts based on the particular gateway used; (b) dynamic risk tools to facilitate investigation of suspicious activity, including counterparty reporting, flow of funds reporting, account flagging of suspicious accounts, and degrees of separation reporting; and (c) other reports of protocol-wide activity regarding any unlawful activity.

11. Funds Travel Rule and Funds Transfer Rule:

XRP II and the Ripple Trade MSB will ensure, or continue to ensure, that all transactions made using XRP II, Ripple Trade, or Ripple Wallet will be, or will continue to be, in compliance with the Funds Transfer Rule and the Funds Travel Rule.