UNITED STATES OF AMERICA
CONSUMER FINANCIAL PROTECTION BUREAU

ADMINISTRATIVE PROCEEDING
File No. 2016-CFPB-0007

In the Matter of: **Dwolla, Inc.**	**CONSENT ORDER**

The Consumer Financial Protection Bureau (Bureau) has reviewed certain acts and practices of Dwolla, Inc. (Respondent, as defined below) and has identified the following law violations: deceptive acts and practices relating to false representations regarding Respondent's data-security practices in violation of Sections 1031(a) and 1036(a)(1) of the Consumer Financial Protection Act of 2010 (CFPA), 12 U.S.C. §§ 5531(a), 5536(a)(1). Under Sections 1053 and 1055 of the CFPA, 12 U.S.C. §§ 5563, 5565, the Bureau issues this Consent Order (Consent Order).

I
Jurisdiction

1. The Bureau has jurisdiction over this matter under Sections 1053 and 1055 of the CFPA, 12 U.S.C. §§ 5563 and 5565.

II
Stipulation

2. Respondent has executed a "Stipulation and Consent to the Issuance of a Consent Order," dated February 24, 2016 (Stipulation), which is incorporated by reference and is accepted by the Bureau. By this Stipulation, Respondent has consented to the issuance of this Consent Order by the Bureau under Sections 1053 and 1055 of the CFPA, 12 U.S.C. §§ 5563 and 5565, without admitting or denying any of the findings of fact or conclusions of law, except that Respondent admits the facts necessary to establish the Bureau's jurisdiction over Respondent and the subject matter of this action.

III
Definitions

3. The following definitions apply to this Consent Order:
   a. "Account "or "Dwolla account" means a Member's designated portion of a pooled account held at a partner bank or credit union that is used to conduct funds transfers through the Dwolla network.
   b. "Advertisement" means any statement, illustration, depiction, or promotional material that is designed to effect a sale or create interest in goods or services, regardless of where it appears.
   c. "Application" or "app" means a mobile or online program or software used to provide Members access to their Dwolla accounts and to facilitate funds transfers through the Dwolla network.
   d. "Board" means Respondent's duly-elected and acting Board of Directors.
   c. "Effective Date" means the date on which the Consent Order is issued.

d. "Enforcement Director" means the Assistant Director of the Office of Enforcement for the Consumer Financial Protection Bureau, or his/her delegate.

e. "Member" means a customer of Respondent holding a Dwolla account.

f. "Network" means the electronic instrument designed and supported by Respondent or its third party vendor(s) which allows a Member the ability to access his or her Dwolla account through Respondent's website or through individual applications designed for that purpose.

g. "Related Consumer Action" means a private action by or on behalf of one or more consumers or an enforcement action by another governmental agency brought against Respondent based on substantially the same facts as described in Section IV of this Consent Order.

h. "Respondent" means Dwolla, Inc., and it successors and assigns.

i. "Risk Assessment" means a written analysis in which an organization assesses the internal and external risks that could result in the compromise of sensitive consumer information and the sufficiency of any safeguards in place to control those risks.

IV
Bureau Findings and Conclusions

The Bureau finds the following:

4. Respondent is a Delaware corporation, with its principal place of business in Des Moines, Iowa.

5. Respondent is a "covered person" under the CFPA as that term is defined by 12 U.S.C. § 5481(6).
6. Respondent launched services in Iowa on December 1, 2009; in California on April 5, 2010; and nationally on December 1, 2010.
7. Respondent's payment network allows a consumer to become a Member by registering for a Dwolla account at Dwolla.com. A Member can then access his or her Dwolla account through the Dwolla website or through individual applications. Members can direct Respondent to effect a transfer of funds to the Dwolla account of another consumer or merchant. The funds for the transfer can come either from funds stored in the consumer's Dwolla account or a personal bank account linked to the consumer's Dwolla account.
8. In order to open a Dwolla account, consumers must submit their name, address, date of birth, telephone number, and Social Security number.
9. In order to link a bank account to a Dwolla account, consumers must submit a bank account number and routing number.
10. In order to transfer funds using a Dwolla account, consumers must enter a username, password, and a unique 4-digit PIN.
11. Respondent stores consumers' sensitive personal information, including the information supplied to Respondent described in Paragraphs 8-10.
12. Respondent holds consumers' funds in a single, pooled account at Veridian Credit Union, an Iowa-chartered, federally-insured credit union, or Compass Bank, a federally-insured bank.

13. Respondent has been collecting and storing consumers' sensitive personal information and providing a platform for financial transactions since December 1, 2009.

14. As of May 2015, Respondent had approximately 653,000 Members and had transferred as much as $5,000,000 per day.

Findings and Conclusions as to Deceptive Data-Security Representations

15. From January 2011 to March 2014, Respondent represented, or caused to be represented, expressly or by implication, to consumers that Respondent employs reasonable and appropriate measures to protect data obtained from consumers from unauthorized access, as detailed below.

16. Respondent represented to consumers that its network and transactions were "safe" and "secure."

17. On its website, Respondent represented that "Dwolla empowers anyone with an internet connection to safely send money to friends or businesses."

18. Respondent's website stated that Dwolla transactions were "safer [than credit cards] and less of a liability for both consumers and merchants."

19. On its website or in direct communications with consumers, Respondent made the following representations indicating that its data-security practices met or exceeded industry standards:

    a. Dwolla 's data-security practices "exceed industry standards," or "surpass industry security standards";

    b. Dwolla "sets a new precedent for the industry for safety and security";

    c. Dwolla stores consumer information "in a bank-level hosting and security environment"; and

d. Dwolla encrypts data "utilizing the same standards required by the federal government."

20. On its website or in direct communications with consumers, Respondent made the following representations regarding its encryption and data-security measures:

a. "All information is securely encrypted and stored";

b. "100% of your info is encrypted and stored securely";

c. Dwolla encrypts "all sensitive information that exists on its servers";

d. Dwolla uses "industry standard encryption technology";

e. Dwolla "encrypt[s] data in transit and at rest";

f. "Dwolla's website, mobile applications, connection to financial institutions, back end, and even APIs use the latest encryption and secure connections"; and

g. Dwolla is "PCI compliant".

21. The Payment Card Industry (PCI) Security Standards Council is an open global forum that issues the data-security compliance standards for cardholder data adopted by some of the world's largest payment card networks, including American Express, MasterCard, and Visa.

22. Respondent represented to consumers that its transactions, servers, and data centers were compliant with the standards set forth by the PCI Security Standards Council.

23. In fact, Respondent failed to employ reasonable and appropriate measures to protect data obtained from consumers from unauthorized access.

24. In fact, Respondent's data-security practices did not "surpass" or "exceed" industry standards.

25. In fact, Respondent did not encrypt all sensitive consumer information in its possession at rest.

26. In fact, Respondent's transactions, servers, and data centers were not PCI compliant.

27. In particular, Dwolla failed to:

    a. adopt and implement data-security policies and procedures reasonable and appropriate for the organization;

    b. use appropriate measures to identify reasonably foreseeable security risks;

    c. ensure that employees who have access to or handle consumer information received adequate training and guidance about security risks;

    d. use encryption technologies to properly safeguard sensitive consumer information; and

    e. practice secure software development, particularly with regard to consumer-facing applications developed at an affiliated website, Dwollalabs.

Data Security Policies and Procedures

28. From its launch until at least September 2012, Respondent did not adopt or implement reasonable and appropriate data-security policies and procedures governing the collection, maintenance, or storage of consumers' personal information.

29. From its launch until at least October 2013, Respondent did not adopt or implement a written data-security plan to govern the collection, maintenance, or storage of consumers' personal information.

Risk Assessments

30. Respondent also failed to conduct adequate, regular risk assessments to identify reasonably foreseeable internal and external risks to consumers' personal information, or to assess the safeguards in place to control those risks.

31. Respondent conducted its first comprehensive risk assessment in mid-2014.

Employee Training

32. Until at least December 2012, Respondent's employees received little to no data-security training on their responsibilities for handling and protecting the security of consumers' personal information.

33. Respondent did not hold its first mandatory employee training on data security until mid-2014.

34. In December 2012, Respondent hired a third party auditor to perform the first penetration test of Dwolla.com. In that test, a phishing e-mail attack was distributed to Respondent's employees that contained a suspicious URL link. Nearly half of Respondent's employees opened the e-mail, and of those, 62% of employees clicked on the URL link. Of those that clicked the link, 25% of employees further attempted to register on the phishing site and provided a username and password.

35. Dwolla failed to address the results of this test or educate its personnel about the dangers of phishing.

36. Dwolla did not conduct its first mandatory employee data-security training until mid-2014.

Encryption

37. Relevant industry standards require encryption of sensitive data.

38. In numerous instances, Respondent stored, transmitted, or caused to be transmitted the following consumer personal information without encrypting that data:

    a. first and last names;

    b. mailing addresses;

    c. Dwolla 4-digit PINS;

    d. Social Security numbers;

    e. Bank account information; and

    f. digital images of driver's licenses, Social Security cards and utility bills.

39. Dwolla also encouraged consumers to submit sensitive information via e-mail in clear text, including Social Security numbers and scans of driver's licenses, utility bills, and passports, in order to expedite the registration process for new users.

Testing Software

40. In July 2012, Respondent hired a software development manager in Iowa who began to establish and implement secure software development practices to govern Respondent's software development operations.

41. At the same time, Respondent operated an alternative software development operation, Dwollalabs.com (Dwollalabs).

42. The software developer leading Dwollalabs software development had no data-security training.

43. The software development that occurred at Dwollalabs did not comply with the security practices that Respondent had implemented to govern the company's software development operations.

44. Respondent created applications through this software developer and released those applications to the public on Dwollalabs.com.

45. Sensitive consumer data was stored on Dwollalabs.com and on its apps.

46. Respondent failed to test the security of the apps on Dwollalabs.com prior to releasing the apps to the public to ensure that consumers' information was protected.

47. These apps included #Dwolla, MassPay, Dwolla IOS app, and Dwolla for Windows.

48. Respondent did not conduct risk assessments or penetration tests on Dwollalabs.com.

49. Respondent's representations regarding its data-security practices, as described in Paragraphs 15-22, were likely to mislead a reasonable consumer into believing that Dwolla had incorporated reasonable and appropriate data-security practices when it had not.

50. Respondent's representations were material because they were likely to affect a consumer's choice or conduct regarding whether to become a member of Dwolla's network.

51. Thus, Dwolla's practices, as described in Paragraphs 15-22, constitute deceptive acts or practices in violation of the CFPA, 12 U.S.C. §§ 5531(a) and 5536(a)(1)(B).

ORDER

V

Conduct Provisions

IT IS ORDERED, under sections 1053 and 1055 of the CFPA, that:

52. Respondent's officers, agents, servants, employees, and attorneys who have actual notice of this Consent Order, whether acting directly or indirectly, may not violate sections 1031(a) and 1036(a)(1) of the CFPA, 12 U.S.C. §§ 5531(a), 5536(a)(1), in connection with the marketing, advertising, promotion or administration of its electronic payment networks and associated systems, platforms and accounts, as follows and must take the following affirmative actions:

    a. Respondent's officers, agents, servants, employees, and attorneys who have actual notice of this Consent Order, whether acting directly or indirectly, in connection with the marketing, advertising, promotion or administration of its electronic payment networks and associated systems, platforms and accounts, are restrained and enjoined from misrepresenting, or assisting others in misrepresenting, expressly or by implication, the data-security practices implemented by Respondent, including with regard to its data storage or encryption practices, PCI compliance, or its adherence to any relevant data-security standard or best practices.

    b. Respondent must, to the extent not already in place, adopt and implement reasonable and appropriate data-security measures to protect consumers' personal information on its computer networks and applications.

c. Respondent must enact the following measures to improve the safety and security of its operations and the consumer information that is stored on, or transmitted through, its network(s):

   i. establish, implement, and maintain a written, comprehensive data-security plan that is reasonably designed to protect the confidentiality, integrity, and availability of sensitive consumer information; the plan must contain administrative, technical, and physical safeguards appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities, and the sensitivity of the personal information collected about consumers;

   ii. adopt and implement reasonable and appropriate data-security policies and procedures;

   iii. designate a qualified person to coordinate and be accountable for the data-security program;

   iv. conduct data-security risk assessments twice annually of each area of relevant operation to identify internal and external risks to the security, confidentiality, and integrity of Respondent's network, systems, or apps, and to consumers' sensitive consumer information stored by Respondent, and to assess the sufficiency of any safeguards in place to control these risks;

   v. evaluate and adjust the data-security program in light of the results of the risk assessments and monitoring required by this Consent Order;

   vi. conduct regular, mandatory employee training on a) the Company's data-security policies and procedures; b) the safe handling of

consumers' sensitive personal information; and c) secure software design, development and testing.

vii. develop, implement, and update, as required, security patches to fix any security vulnerabilities identified in any web or mobile application;

viii. develop, implement and maintain an appropriate method of customer identity authentication at the registration phase and before effecting a funds transfer;

ix. develop, implement, and maintain reasonable procedures for the selection and retention of service providers capable of maintaining security practices consistent with this Consent Order and require service providers by contract to implement and maintain appropriate safeguards; and

x. obtain an annual data-security audit from an independent, qualified third-party, using procedures and standards generally accepted in the profession, as described in Section VI.

VI
Audit Report and Compliance Plan

IT IS FURTHER ORDERED that:

53. Within 30 days of the Effective Date, Respondent must secure and retain one or more qualified, independent person(s), with specialized experience in data security, and acceptable to the Enforcement Director, to conduct an annual data-security audit of Respondent's data-security practices. Within 10 days of the Effective Date, Respondent must identify the qualified, independent person and

the person's relevant qualifications to the Enforcement Director for his or her non-objection.

54. The purpose of the data-security audit must be to validate the effectiveness of the periodic risk assessments conducted under Paragraph 52(c)(iv) in identifying any internal or external risks to the security, confidentiality, and integrity of the sensitive consumer information obtained by Respondent from consumers and to verify that the Company has implemented reasonable and appropriate risk mitigation activities to sufficiently safeguard against any identified risks. The data-security audit must include a review of Respondent's compliance with the data-security measures required by this Consent Order.

55. Within 180 days of the Effective Date, the qualified person(s) must prepare a written report detailing the findings of the audit (the Audit Report or AR), and provide the AR to the Board.

56. Within 30 days of receiving the AR , the Board must:

    a. Develop a plan (Compliance Plan) to: (i) correct any deficiencies identified, and (ii) implement any recommendations or explain in writing why a particular recommendation is not being implemented; and

    b. Submit the AR and the Compliance Plan to the Enforcement Director.

57. Respondent must conduct the independent data-security audit and prepare an AR on an annual basis.

58. The Enforcement Director will have the discretion to make a determination of non-objection to the Compliance Plan or to direct Respondent to revise it. If the Enforcement Director directs Respondent to revise the Compliance Plan, the Board

must make the requested revisions and resubmit the Compliance Plan to the Enforcement Director within 20 days.

59. After receiving notification that the Enforcement Director has made a determination of non-objection to the Compliance Plan, Respondent must implement and adhere to the steps, recommendations, deadlines, and timeframes outlined in the Compliance Plan.

VII
Role of the Board

IT IS FURTHER ORDERED that:

60. The Board must review all submissions (including plans, reports, programs, policies, and procedures) required by this Consent Order prior to submission to the Bureau.

61. Although this Consent Order requires Respondent to submit certain documents for the review or non-objection by the Enforcement Director, the Board will have the ultimate responsibility for proper and sound management of Respondent and for ensuring that it complies with Federal consumer financial law and this Consent Order.

62. In each instance that this Consent Order requires the Board to ensure adherence to, or perform certain obligations of Respondent, the Board must:

    a. Authorize whatever actions are necessary for Respondent to fully comply with the Consent Order;

    b. Require timely reporting by management to the Board on the status of compliance obligations; and

c. Require timely and appropriate corrective action to remedy any material non-compliance with any failures to comply with Board directives related to this Section.

VIII
Order to Pay Civil Money Penalties

IT IS FURTHER ORDERED that:

63. Under section 1055(c) of the CFPA, 12 U.S.C. § 5565(c), by reason of the violations of law described in Section IV of this Consent Order, and taking into account the factors in 12 U.S.C. § 5565(c)(3), Respondent must pay a civil money penalty of $100,000 to the Bureau.

64. Within 10 days of the Effective Date, Respondent must pay the civil money penalty by wire transfer to the Bureau or to the Bureau's agent in compliance with the Bureau's wiring instructions.

65. The civil money penalty paid under this Consent Order will be deposited in the Civil Penalty Fund of the Bureau as required by section 1017(d) of the CFPA, 12 U.S.C. § 5497(d).

66. Respondent must treat the civil money penalty paid under this Consent Order as a penalty paid to the government for all purposes. Regardless of how the Bureau ultimately uses those funds, Respondent may not:

    a. Claim, assert, or apply for a tax deduction, tax credit, or any other tax benefit for any civil money penalty paid under this Consent Order; or

    b. Seek or accept, directly or indirectly, reimbursement or indemnification from any source, including but not limited to payment made under any insurance policy, with regard to any civil money penalty paid under this Consent Order.

IX
Additional Monetary Provisions

IT IS FURTHER ORDERED that:

67. In the event of any default on Respondent's obligations to make payment under this Consent Order, interest, computed under 28 U.S.C. § 1961, as amended, will accrue on any outstanding amounts not paid from the date of default to the date of payment, and will immediately become due and payable.

68. Respondent must relinquish all dominion, control, and title to the funds paid to the fullest extent permitted by law and no part of the funds may be returned to Respondent.

69. Under 31 U.S.C. § 7701, Respondent, unless it already has done so, must furnish to the Bureau its taxpayer identifying numbers, which may be used for purposes of collecting and reporting on any delinquent amount arising out of this Consent Order.

70. Within 30 days of the entry of a final judgment, Consent Order, or settlement in a Related Consumer Action, Respondent must notify the Enforcement Director of the final judgment, Consent Order, or settlement in writing. That notification must indicate the amount of redress, if any, that Respondent paid or is required to pay to consumers and describe the consumers or classes of consumers to whom that redress has been or will be paid.

X
Reporting Requirements

IT IS FURTHER ORDERED that:

71. Respondent must notify the Bureau of any development that may affect compliance obligations arising under this Consent Order, including but not limited to, a dissolution, assignment, sale, merger, or other action that would result in the emergence of a successor company; the creation or dissolution of a subsidiary, parent, or affiliate that engages in any acts or practices subject to this Consent Order; the filing of any bankruptcy or insolvency proceeding by or against Respondent; or a change in Respondent's name or address. Respondent must provide this notice, if practicable, at least 30 days before the development, but in any case no later than 14 days after the development.

72. Respondent must report any change in the information required to be submitted under Paragraph 71 at least 30 days before the change or as soon as practicable after learning about the change, whichever is sooner.

73. Within 90 days of the Effective Date, and again one year after the Effective Date, Respondent must submit to the Enforcement Director an accurate written compliance progress report (Compliance Report) that has been approved by the Board, which, at a minimum:

    a. Describes in detail the manner and form in which Respondent has complied with this Consent Order; and

    b. Attaches a copy of each Order Acknowledgment obtained under Section XI, unless previously submitted to the Bureau.

XI
Order Distribution and Acknowledgment

IT IS FURTHER ORDERED that,

74. Within 30 days of the Effective Date, Respondent must deliver a copy of this Consent Order to each of its board members and executive officers, as well as to any managers, employees, service providers, or other agents and representatives who have responsibilities related to the subject matter of the Consent Order.

75. For 5 years from the Effective Date, Respondent must deliver a copy of this Consent Order to any business entity resulting from any change in structure referred to in Section X, any future board members and executive officers, as well as to any managers, employees, service providers, or other agents and representatives who will have responsibilities related to the subject matter of the Consent Order before they assume their responsibilities.

76. Respondent must secure a signed and dated statement acknowledging receipt of a copy of this Consent Order, ensuring that any electronic signatures comply with the requirements of the E-Sign Act, 15 U.S.C. § 7001 *et seq.*, within 30 days of delivery, from all persons receiving a copy of this Consent Order under this Section.

XII
Recordkeeping

IT IS FURTHER ORDERED that

77. Respondent must create, or if already created, must retain for at least 5 years from the Effective Date, the following business records:

    a. All documents and records necessary to demonstrate full compliance with

each provision of this Consent Order, including all submissions to the Bureau.

b. Copies of all policies and procedures, training materials, risk assessments, advertisements, and other marketing materials, related to data security or the protection of sensitive consumer information, including any such materials used by a third party on behalf of Respondent.

c. All consumer complaints and refund requests (whether received directly or indirectly, such as through a third party) that relate to data security, and any responses to those complaints or requests.

d. Records showing, for each employee with responsibilities related data security or information privacy, that person's: name; telephone number; email, physical, and postal address; job title or position; dates of service; and, if applicable, the reason for termination.

e. Records showing, for each service provider providing services related to data security or information privacy, the name of a point of contact, and that person's telephone number; email, physical, and postal address; job title or position; dates of service; and, if applicable, the reason for termination.

78. Respondent must retain the documents identified in Paragraph 77 for at least five years.

79. Respondent must make the documents identified in Paragraph 77 available to the Bureau upon the Bureau's request.

XIII
Notices

IT IS FURTHER ORDERED that:

80. Unless otherwise directed in writing by the Bureau, Respondent must provide all submissions, requests, communications, or other documents relating to this Consent Order in writing, with the subject line, "*In re Dwolla, Inc.*, File No. 2016-CFPB-0007," and send them either:

    a. By overnight courier (not the U.S. Postal Service), as follows:

        Assistant Director for Enforcement
        Consumer Financial Protection Bureau
        ATTENTION: Office of Enforcement
        1625 EYE Street, N.W.
        Washington D.C. 20006; or

    b. By first-class mail to the below address and contemporaneously by email to Enforcement_Compliance@cfpb.gov:

        Assistant Director for Enforcement
        Consumer Financial Protection Bureau
        ATTENTION: Office of Enforcement
        1700 G Street, N.W.
        Washington D.C. 20552

XIV
Compliance Monitoring

IT IS FURTHER ORDERED that, to monitor Respondent's compliance with this Consent Order:

81. Within 30 days of receipt of a written request from the Bureau, Respondent must submit additional Compliance Reports or other requested information, which must be made under penalty of perjury; provide sworn testimony; or produce documents.

82. Respondent must permit Bureau representatives to interview any employee or other person affiliated with Respondent who has agreed to such an interview. The person interviewed may have counsel present.

83. Nothing in this Consent Order will limit the Bureau's lawful use of civil investigative demands under 12 C.F.R. § 1080.6 or other compulsory process.

84. For the duration of the Consent Order in whole or in part, Respondent agrees to be subject to the Bureau's supervisory authority under 12 U.S.C. § 5514. Consistent with 12 C.F.R. § 1091.111, Respondent may not petition for termination of supervision under 12 C.F.R. § 1091.113.

XV
Modifications to Non-Material Requirements

IT IS FURTHER ORDERED that:

85. Respondent may seek a modification to non-material requirements of this Consent Order (*e.g.*, reasonable extensions of time and changes to reporting requirements) by submitting a written request to the Enforcement Director.

86. The Enforcement Director may, in his/her discretion, modify any non-material requirements of this Consent Order (*e.g.*, reasonable extensions of time and changes to reporting requirements) if he/she determines good cause justifies the modification. Any such modification by the Enforcement Director must be in writing.

XVI
Administrative Provisions

87. The provisions of this Consent Order do not bar, estop, or otherwise prevent the Bureau, or any other governmental agency, from taking any other action against Respondent, except as described in Paragraph 88.

88. The Bureau releases and discharges Respondent from all potential liability for law violations that the Bureau has or might have asserted based on the practices described in Section IV of this Consent Order, to the extent such practices occurred before the Effective Date and the Bureau knows about them as of the Effective Date. The Bureau may use the practices described in this Consent Order in future enforcement actions against Respondent or its affiliates, including, without limitation, to establish a pattern or practice of violations or the continuation of a pattern or practice of violations or to calculate the amount of any penalty. This release does not preclude or affect any right of the Bureau to determine and ensure compliance with the Consent Order, or to seek penalties for any violations of the Consent Order.

89. This Consent Order is intended to be, and will be construed as, a final Consent Order issued under section 1053 of the CFPA, 12 U.S.C. § 5563, and expressly does not form, and may not be construed to form, a contract binding the Bureau or the United States.

90. This Consent Order will terminate 5 years from the Effective Date or 5 years from the most recent date that the Bureau initiates an action alleging any violation of the Consent Order by Respondent. If such action is dismissed or the relevant adjudicative body rules that Respondent did not violate any provision of the

Consent Order, and the dismissal or ruling is either not appealed or upheld on appeal, then the Consent Order will terminate as though the action had never been filed. The Consent Order will remain effective and enforceable, except to the extent that, and until such time as, any provisions of this Consent Order has been amended, suspended, waived, or terminated in writing by the Bureau or its designated agent.

91. Calculation of time limitations will run from the Effective Date and be based on calendar days, unless otherwise noted.

92. Should Respondent seek to transfer or assign all or part of its operations that are subject to this Consent Order, Respondent must, as a condition of sale, obtain the written agreement of the transferee or assignee to comply with all applicable provisions of this Consent Order.

93. The provisions of this Consent Order will be enforceable by the Bureau. For any violation of this Consent Order, the Bureau may impose the maximum amount of civil money penalties allowed under section 1055(c) of the CFPA, 12 U.S.C. § 5565(c). In connection with any attempt by the Bureau to enforce this Consent Order in federal district court, the Bureau may serve Respondent wherever Respondent may be found and Respondent may not contest that court's personal jurisdiction over Respondent.

94. This Consent Order and the accompanying Stipulation contain the complete agreement between the parties. The parties have made no promises, representations, or warranties other than what is contained in this Consent Order and the accompanying Stipulation. This Consent Order and the accompanying

Stipulation supersede any prior oral or written communications, discussions, or understandings.

95. Nothing in this Consent Order or the accompanying Stipulation may be construed as allowing Respondent, its Board, officers, or employees to violate any law, rule, or regulation.

IT IS SO ORDERED, this 27th day of February, 2016.

Richard Cordray

Richard Cordray
Director
Consumer Financial Protection Bureau