UNITED STATES OF AMERICA
CONSUMER FINANCIAL PROTECTION BUREAU

ADMINISTRATIVE PROCEEDING
File No. 2023-CFPB-0005

In the Matter of: **ACI WORLDWIDE CORP, AND ACI PAYMENTS, INC.**	**CONSENT ORDER**

The Consumer Financial Protection Bureau (Bureau) has reviewed conduct of respondents ACI Worldwide Corp. and ACI Payments Inc. (collectively, ACI or Respondent as defined below) in relation to the more than 1.4 million erroneous ACH Entries which ACI initiated on April 23, 2021, totaling more than $2.3 billion and which impacted 478,568 consumer bank accounts (April 2021 Incident). The Bureau has also reviewed the relevant information security practices and controls that Respondent maintained to govern Sensitive Consumer Financial Information (SCFI) at the time of the April 2021 Incident and has identified the following law violations: Respondent engaged in unfair acts and practices by failing to adopt and enforce reasonable and appropriate information

security practices that put its Speedpay platform operations, and the SCFI Respondent processed or maintained, at risk which directly led to the April 2021 Incident. Although ACI was able to offset the ACH Entries before funds were debited from the majority of consumers' accounts, the erroneous ACH Entries ACI initiated during the April 2021 Incident constituted unfair acts or practices which nonetheless caused substantial consumer harm including significant frustration, confusion, and monetary loss in violation of the Consumer Financial Protection Act (CFPA), 12 U.S.C. §§ 5531(a), 5536(a)(1), 5564. Some of these ACH Entries also violated the Electronic Fund Transfer Act (EFTA) 15 U.S.C. § 1693e(a), and its implementing Regulation E, 12 C.F.R. § 1005.10(b). Under §§ 1053 and 1055 of the Consumer Financial Protection Act of 2010 (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 §§ 1053 and 1055 of the CFPA, 12 U.S.C. §§ 5563 and 5565. The Bureau has authority to enforce EFTA and its implementing Regulation E, 12 U.S.C. §§ 5531(a), 5536(a)(1), 5564; 15 U.S.C. § 1693e(a); 12 C.F.R. § 1005.10(b).

II.

Stipulation

2. Respondent has executed a "Stipulation and Consent to the Issuance of a Consent Order," dated June 20, 2023 (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 §§ 1053 and 1055 of the CFPA, 12 U.S.C. §§ 5563, 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. "ACH Entry" means an electronic funds transfer payment instruction processed through the ACH Network in order to push a credit to a designated account or pull a debit from a designated account.

   b. "Affected Consumers" means consumers whose bank accounts received erroneous ACH Entries which they did not approve and also suffered a reduction in their available balance as a result of the April 2021 Incident.

c. "Availability" means the existence of effective technological and human internal controls that ensure the timely and reliable access to and use of information.

d. "Board" means ACI Worldwide Corp's duly elected and acting Board of Directors.

e. "CISO" means Chief Information Security Officer.

f. "Confidentiality" means the existence of effective technological and human internal controls that preserve authorized restrictions on access and disclosure, including means for protecting consumer privacy and proprietary information.

g. "Effective Date" means the date on which the Consent Order is entered on the administrative docket.

h. "Electronic Fund Transfer (EFT)" means any transfer of funds that is initiated through an electronic terminal, telephone, computer, or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account.

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

j. "Information Security Research Community" means the community of practitioners, academics and other researchers regularly engaged in the study of information security for, among other things, the purpose of building shared knowledge regarding information security, as such work is publicly shared through:

   i. Major general interest media outlets and technology industry publications;

   ii. Governmental security advisories, guidelines, and notifications such as those issued by the Cybersecurity & Infrastructure Security Agency, NIST, or other relevant entities; and

   iii. Presentations of major information security conferences.

k. "Integrity" means the existence of effective technological and human internal controls that guard against improper modification or destruction of information.

l. "Originating Depository Financial Institution or ODFI" means the financial institution which delivers Automated Clearing House (ACH) entries directly or indirectly into the ACH network to execute funds transfers.

m. "Originator" means a person that has authorized an ODFI (directly or through a Third-Party Sender) to transmit a credit entry or debit entry to

the Receiver's account at the RDFI, with the funds to be debited or credited to the Originator's account at a future date.

n. "Receiving Depository Financial Institution" or "RDFI" means the financial institution that holds the account of the Receiver identified in an ACH Entry and typically posts the ACH Entries to the Receiver's account at the RDFI based on the information contained in the ACH file.

o. "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.

p. "Reasonable Security" means the adoption and enforcement of information security policies and human and technical internal control measures that are technically substantiated by the latest knowledge, widely held within the Information Security Research Community, and that are:

    i. Documented in human readable format by internal corporate threat modeling documents, incident response policies, and other relevant documentation; and

    ii. Sufficient to defend and ensure the Confidentiality, Integrity, and Availability of SCFI and Respondent's systems.

q. "Respondent" means ACI Worldwide Corp, ACI Payments Inc., and their successors and assigns.

r. "Sensitive Consumer Financial Information" or "SCFI" means information connectable to a consumer:

   i. That a consumer provides to obtain a consumer financial product or service;

   ii. About a consumer resulting from any transaction involving a consumer financial product or service involving Respondent; or

   iii. That is otherwise obtained, derived, or generated about a consumer in connection with providing a consumer financial product or service.

s. "Service Provider" means any person that provides a material service to a Respondent in connection with the offering or provision by Respondent of a consumer financial product or service.

t. "Synthetic Data" means data which is artificially generated that mimics but does not contain real consumer records.

u. "Third-Party Sender" is a third-party service provider which acts on behalf of an Originator as an intermediary in transmitting entries between an Originator and an ODFI.

IV.

Bureau Findings and Conclusions

The Bureau finds the following:

4. Respondent ACI Worldwide Corp. (ACI Corp.) is a Nebraska corporation, with its headquarters in Elkhorn, Nebraska.

5. Respondent ACI Payments, Inc. (ACI Payments) is a Delaware corporation and a wholly owned subsidiary of ACI Worldwide Corp., with its principal place of business in Elkhorn, Nebraska.

6. ACI Payments transacts business throughout the United States.

7. ACI Payments provides payment processing services for use by consumers and is a service provider to nationwide mortgage servicers. Therefore, ACI Payments is a "covered person" under the CFPA. 12 U.S.C. § 5481(6)(A), (15)(A)(vii), (26)(A).

8. ACI Corp. is a "controlling shareholder" of ACI Payments and is therefore a "related person" under the CFPA. 12 U.S.C. § 5481(25)(C)(i). Therefore, it is also a "covered person" for purposes of the statute. 12 U.S.C. § 5481(25)(B).

9. ACI Corp. has direct or indirect control over ACI Payments and shares integrated services with respect to core IT and other operational aspects of the enterprise pursuant to intercompany agreements.

10. At all times relevant to this Consent Order, Respondent's interconnected companies operated as a "common enterprise." Accordingly, ACI Corp., and ACI Payments are jointly and severally liable for the acts and practices referenced below.

ACI's Business

11. Respondent develops, markets, installs, and supports software products and services that facilitate electronic payments.

12. Respondent is a Third-Party Sender that offers various payment services to consumers across a wide range of industries, processing over 500 million bill payment transactions annually. Its clients include entities from a wide range of industries including one of the nation's largest mortgage servicers.

13. To provide payment services, Respondent collects, processes, and stores, large amounts of SCFI, including names, bank account numbers, bank routing numbers, and payment amounts.

14. ACI Payments' Speedpay platform is part of its suite of electronic bill payment services.

15. ACI Payments acquired Speedpay in May 2019 from Western Union.

16. ACI took over operation of the Speedpay platform on March 1, 2021, after the expiration of a transaction services agreement with Western Union on February 28, 2021.

17. Speedpay uses the Automated Clearing House Network (ACH Network) to electronically transfer funds for the purpose of providing its payment processing services.

18. At all times relevant to this Consent Order, Mr. Cooper, a mortgage servicer for over four million mortgage loans (Mortgage Company) was one of ACI Payments' largest customers.

19. Consumers with mortgage loans serviced by the Mortgage Company could schedule their monthly mortgage payments by authorizing a one-time electronic fund transfer or preauthorizing recurring electronic fund transfers from their individual bank accounts on a scheduled date. The Mortgage Company's borrowers who chose to use this service provided bank account information to the Mortgage Company, which transmitted it to ACI.

20. As part of its bill payment service, ACI prepares files containing ACH Entries necessary to process each mortgage payment and periodically sends these files to its ODFI. The ODFI then submits the ACH files to its ACH operator, which transmits the files to the Mortgage Company's

borrowers' banks, the RDFIs, to debit or credit the relevant amounts out of or into the borrowers' accounts.

The April 2021 Incident

21. On April 23, 2021, ACI initiated more than 1.4 million erroneous ACH Entries that were not approved by consumers. These 1,431,377 debit entries and 1,444 credit entries transmitted electronic mortgage payment instructions totaling over $2.3 billion to the bank accounts of 478,568 Mortgage Company's borrowers. As a result, many of these borrowers unknowingly had multiple debits for monthly mortgage payments scheduled to hit their bank account on a single day.

22. This incident resulted from ACI's lack of Reasonable Security sufficient to, among other things: (1) securely segregate Speedpay's testing environment (where ACI maintains databases which contain data for use in testing and development of software before it is used in a production environment); (2) detect and prevent the transmission of ACH test files containing SCFI to an ACI contractor; (3) detect and prevent an ACI contractor from improperly creating ACH test files using SCFI; and (4) detect and prevent the transmission of those ACH files into the ACH Network.

23. On or about April 23, 2021, ACI contractors conducted performance tests on ACI's Speedpay platform that involved simulating actual ACH Entry processing. ACI contractors handling the testing project did not use "dummy" consumer data (*i.e.,* data that do not contain SCFI) or ensure that any consumer data in the data files used for testing were scrubbed of SCFI, contrary to ACI policy.

24. Instead, ACI contractors circumvented ACI policies and processes related to the access and use of SCFI, and were able to obtain and use actual, unaltered, SCFI that ACI previously obtained for legitimate debit and credit transactions for the Mortgage Company's borrowers.

25. No ACI employee or contractor checked to ensure that SCFI was removed from the files before the tests were run.

26. Therefore, the tests produced executable ACH files even though they were not intended to bring about actual ACH transactions.

27. The Speedpay platform recognized the test files as authentic and containing legitimate ACH Entries which instructed consumers' banks to debit or credit the Mortgage Company's borrowers' accounts accordingly.

28. This circumvention of ACI's policy regarding the handling of SCFI, in addition to the failure to segregate internal production and testing

environments, directly resulted in ACI erroneously transmitting 1,432,821 ACH Entries to its ODFI.

29. Some of these 1,432,821 ACH Entries resulted in EFTs, and none of them were authorized by the borrowers to whose accounts they were directed.

30. The ODFI was unaware that the ACH files it received were not ordinary files meant for processing, and ultimately submitted them into the ACH Network impacting nearly 500,000 borrower bank accounts beginning on the morning of April 24, 2021.

31. ACI learned of its erroneous ACH Entries on Saturday, April 24, 2021, after the Mortgage Company notified ACI of a growing number of complaints from its borrowers.

32. ACI then sent its ODFI reversing ACH files later that day which were submitted to the ACH Network on Sunday, April 25, 2021. These reversing files included ACH credit entries intended to offset the initial erroneous debit entries, and ACH debit entries intended to offset the initial erroneous credit entries. The initial ACH Entries from April 23, 2021, and the correcting ACH Entries from April 25, 2021, settled on Monday, April 26, 2021.

33. As a result of the erroneous ACH debit entries, some impacted consumer bank accounts were unexpectedly depleted by one or more RDFIs,

depriving Affected Consumers of the use of their funds, including by being prevented from making purchases or completing other legitimate transactions, and many were charged fees, including fees for insufficient funds or overdrawn accounts.

34. Many consumers expended significant time and effort in demanding answers, refunds, and corrections to their accounts from their relevant financial institutions.

Respondent's Deficient Information Security

35. Respondent harmed consumers by failing to implement or enforce information security practices and controls that were appropriate relative to the volume of SCFI it obtains, processes, and stores in connection with its Speedpay bill payment platform. For example:

a. ACI failed to follow appropriate practices regarding the secure segregation of production and non-production environments;

b. ACI failed to implement appropriate data governance controls to prevent the improper use of SCFI;

c. ACI failed to adequately train and oversee contractors who played a critical role in its payment processing operations and had access to SCFI; and

d. ACI failed to implement reasonable and appropriate internal controls to detect violations of its information security protocols.

Respondent Violated EFTA and Regulation E

36. The ACH Entries described in paragraphs 21 to 35 above that resulted in fund transfers to or from a consumer's account are electronic funds transfers (EFTs) under EFTA, 15 USC § 1693, *et seq.*

37. EFTA and its implementing Regulation E require preauthorized EFTs from a consumer's account to be in writing. 15 U.S.C. § 1693e(a); 12 C.F.R. § 1005.10(b).

38. ACI initiated ACH EFTs against consumers' accounts on April 23, 2021, without a valid written authorization for those EFTs that resulted in fund transfers to or from a consumer's account, including by initiating EFTs on days and in amounts that the accountholders had not authorized.

39. ACI's EFTA violations harmed consumers by depriving some consumers of the use of their funds, impacting their ability to pay other expenses, and potentially resulting in fees, such as insufficient funds, overdraft, or late fees.

40. Therefore, ACI violated EFTA, 15 U.S.C. § 1693e(a), and Regulation E, 12 C.F.R. § 1005.10(b).

ACI's EFTA Violations are Violations of the CFPA

41. Section 1036(a)(1)(A) of the CFPA makes it unlawful for covered persons, such as ACI, to "commit any act or omission in violation of a Federal consumer financial law." 12 U.S.C. § 5536(a)(1)(A).

42. EFTA is a "Federal consumer financial law." 12 U.S.C. § 5481(12)(C), (14).

43. By violating EFTA as described in paragraphs 36 to 40, ACI violated the CFPA. 12 U.S.C. § 5536(a)(1)(A).

ACI's Erroneous Processing of ACH Entries Against Consumers' Accounts was Unfair

44. Section 1036(a)(1)(B) of the CFPA prohibits covered persons from engaging "in any unfair, deceptive, or abusive act or practice." 12 U.S.C. §§ 5531, 5536(a)(1)(B). A practice is unfair if the "act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers" and "such injury is not outweighed by countervailing benefits to consumers or competition." 12 U.S.C. § 5531(c).

45. ACI engaged in unfair acts and practices when it erroneously processed ACH Entries meant for the test environment against actual consumer accounts.

46. ACI's acts and practices caused or were likely to cause substantial injury to consumers by erroneously processing ACH payment transactions against their accounts, depriving many consumers of the use of their funds, impacting their ability to pay other expenses, and causing the imposition of fees, such as insufficient funds, overdraft, or late fees.

47. The harm ACI caused or was likely to cause was not reasonably avoidable by consumers. Consumers could not have reasonably anticipated that ACI would initiate multiple ACH Entries against their account without their authorization. Furthermore, once some consumers discovered the transactions had been processed, it was already too late for them to take steps to mitigate the harm.

48. The injury to consumers caused by ACI's acts and practices is not outweighed by countervailing benefits to consumers or competition. There is no benefit to either consumers or competition from having erroneous ACH Entries sent to their financial institutions without their knowledge or permission.

49. Therefore, ACI's processing of these erroneous ACH Entries against consumers' accounts constituted unfair acts or practices in violation of Sections 1031 and 1036 of the CFPA, 12 U.S.C. §§ 5531(a) and (c)(1), and 5536(a)(1)(B).

ACI's Failure to Appropriately Safeguard Consumers' Sensitive Financial Information was Unfair

50. ACI's information security policies and practices were inappropriate for a company that offers millions of consumers services to execute critically important financial transactions and therefore handles massive amounts of SCFI.

51. Among other things, contrary to ACI policy and procedures, ACI's contractors were able to inappropriately use unaltered production data files containing SCFI for testing its Speedpay platform. ACI failed to provide adequate oversight of contractors who had access to such SCFI. ACI also failed to appropriately segregate the Speedpay production environment from its non-production testing environment or properly utilize standard human and technological controls to appropriately manage SCFI.

52. These acts and practices caused or were likely to cause substantial injury to consumers that consumers could not reasonably avoid and that were not outweighed by countervailing benefits to consumers or competition. ACI's deficient information security practices led to ACI Payments erroneously processing 1,432,821 ACH debit and credit Entries on April 23, 2021, and to the fees and charges consumers who received ACH debit Entries suffered as a consequence.

53. Consumers could not reasonably avoid ACI's conduct and could not reasonably anticipate that ACI's information security practices were inadequate to protect against improper use of their SCFI.

54. The injury to consumers was not outweighed by countervailing benefits to consumers or to competition.

55. Therefore, ACI's failure to adopt and enforce Reasonable Security constituted an unfair act or practice in violation of Sections 1031 and 1036 of the CFPA, 12 U.S.C. §§ 5531(a) and (c)(1), and 5536(a)(1)(B).

CONDUCT PROVISIONS

V.

Prohibited Conduct

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

56. Respondent and its officers, agents, servants, employees, and attorneys who have actual notice of this Consent Order, whether acting directly or indirectly, are permanently restrained and enjoined from violating the CFPA, including 12 U.S.C. §§ 5531(a), 5536(a)(1)(B), and EFTA, 15 U.S.C. § 1693, and its implementing Regulation E, 12 C.F.R. § 1005, and shall not offer or provide EFT services in connection with payment processing without taking the following affirmative steps:

a. Obtaining authorization (or requiring its client to obtain such authorization) for ACH debit Entries in compliance with the EFTA for any transfer from the consumer's account; and

b. Adopting appropriate practices, consistent with this Order, to ensure that unauthorized, duplicate, or erroneous ACH Entries can be detected and validated as authentic prior to transmission into the ACH Network for money transmission.

57. Respondent and its officers, agents, servants, employees, and attorneys who have actual notice of this Consent Order, whether acting directly or indirectly, are permanently restrained and enjoined from using SCFI for the purpose of testing or development of software or systems owned or operated by, or on the behalf of, Respondent.

a. However, in the event that a compelling business reason arises necessitating the use of SCFI for testing or development, Respondent shall create an exception report explaining the circumstances of the exception and why other alternatives were not appropriate (SCFI Exception Report). A SCFI Exception Report shall be personally reviewed and authorized by the Qualified Individual (defined below) prior to any use of SCFI for testing and development work.

i. A SCFI Exception Report shall explain the justification for the use of SCFI and how the information will be protected through Reasonable Security measures.

ii. Notwithstanding the above, no SCFI shall be used for purposes of testing or development without first obtaining the consent of each consumer whose sensitive financial information will be used in the applicable testing or development activity.

VI.
Required Conduct

Authorizations

58. Respondent, in connection with processing a consumer electronic payment transaction, must obtain or cause to be obtained proof of a consumer's authorization consistent with all applicable laws, rules, and regulations prior to initiating a consumer electronic payment transaction.

Information Security Program

59. Respondent must enforce, and document in human readable form, a program of internal controls to ensure Reasonable Security appropriate to Respondent's size and complexity, the nature and scope of Respondent's activities related to the offering or provision of a consumer financial product or service, and the sensitivity of any consumer information used or

maintained by Respondent (Information Security Program or ISP). The ISP shall require Respondent to:

a. Designate a qualified individual(s) responsible for overseeing, implementing, and enforcing the ISP (Qualified Individual(s)). The Qualified Individual(s) may be employed by ACI, an affiliate, or a service provider. To the extent the requirement in this subparagraph is met using a service provider or an affiliate, Respondent shall:
    i. Retain responsibility for compliance with the Order;
    ii. Retain oversight through the CISO, who shall be responsible for day-to-day direction and oversight of the Qualified Individual(s); and
    iii. Require the service provider or affiliate to maintain an information security program that maintains continuous Reasonable Security in accordance with the requirements of this Order.
b. Periodically (i) perform and document in human readable format threat modeling and risk assessments that consider the sufficiency of the technical and human internal controls in place to maintain Reasonable Security, and (ii) reexamine the reasonably foreseeable internal and external risks to the Confidentiality, Integrity, and Availability of SCFI as required by Reasonable Security.

c. The threat modeling documentation and accompanying risk assessment shall conform with Reasonable Security and shall be written in human readable format and shall include:

   i. The criteria for the evaluation and categorization of identified security risks or threats to Respondent's systems and SCFI;

   ii. Criteria for the assessment of Respondent's Reasonable Security, including the efficacy of the existing controls in the context of the identified risks or threats Respondent faces; and

   iii. Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks.

d. Regularly test or otherwise monitor the effectiveness of internal controls consistent with Reasonable Security.

e. Conduct risk-based annual penetration testing of all critical systems relating to performance of Respondent' services involving SCFI.

f. Evaluate and adjust the ISP on an ongoing basis as required by Reasonable Security.

g. Ensure Reasonable Security including, without limitation, through the development, maintenance and enforcement of policies and procedures to

ensure Respondent's personnel and Service Providers are able to enact the ISP by:

i. Providing ACI personnel with training consistent with the principles of Reasonable Security;

ii. Utilizing qualified information security personnel employed by ACI or an affiliate or Service Provider sufficient to manage Respondent's information security risks and to perform or oversee the ISP;

iii. Providing information security personnel with security updates and training sufficient to defend against relevant security risks; and

iv. Verifying that key information security personnel take steps to maintain current knowledge of measures sufficient to ensure Reasonable Security.

h. Oversee Service Providers, by:

i. Taking necessary steps to select and retain Service Providers that are capable of maintaining Reasonable Security to ensure the Confidentiality, Integrity, and Availability of Respondent's systems and SCFI maintained on or processed by those systems;

ii. Requiring Service Providers, by contract, to implement Reasonable Security; and

iii. Periodically assessing Service Providers based on the risk each presents and their maintenance of their Reasonable Security practices.

i. Require the CISO or Qualified Individual(s) to report in writing, regularly and at least annually, to the Board. The report shall include at a minimum:

i. The overall status of the ISP and Respondent's compliance with the ISP; and

ii. All material matters and findings related to the ISP, including any recommendations for changes in the ISP.

Registration for the Bureau's Consumer Complaint Portal

60. Within 30 days of the Effective Date, ACI Payments Inc. must complete all steps necessary to register for the Bureau's Company Portal, including providing the information required at www.consumerfinance.gov/company-signup and in the Bureau's Company Portal Boarding Form (OMB No. 3170-0054). Respondent, in connection with responding to consumer complaints and inquiries, whether

acting directly or indirectly, are subject to and may not violate § 1034(b) and (c) of the CFPA, 12 U.S.C. §§ 5534(b) and (c).

VII.

Independent Consultant's Report and Compliance Plan

IT IS FURTHER ORDERED that:

61. Within 45 days of the Effective Date, Respondent must secure and retain one or more independent consultants, with specialized experience in information security, and acceptable to the Enforcement Director, to review and validate the implementation of the recommended enhancements made as a result of the internal review of ACI's Third-Party Risk Management (TPRM) or certify that ACI's current information security program and relevant operations comport with Reasonable Security (Independent Review).

62. Within 180 days of the Effective Date, the independent consultant(s) must prepare a written report detailing the methodology utilized to conduct the Independent Review, the information, documentation, and individuals interviewed as part of the Independent Review, the findings and recommendations identified by the consultant, and any other relevant information identified as a result of the Independent Review (the

Independent Consultant Report), and provide the Independent Consultant Report to the CISO and the Board.

63. Within 25 days of receiving the Independent Consultant Report, the Board must:

a. Develop a plan (the Compliance Plan) to correct any deficiencies and implement any recommendations identified by the Consultant Report (or explain in writing why a particular recommendation is not being implemented and how Reasonable Security will be achieved or maintained without implementing the recommendation(s)); and

b. Submit the Independent Consultant Report and the Compliance Plan to the Enforcement Director.

c. In addition to the requirements contained in subsection (a), at a minimum the Compliance Plan must ensure compliance with this Consent Order and:

i. Identify the Qualified Individual(s) by name;

ii. Identify member(s) of the Board by name with primary responsibility for oversight of the Qualified Individual(s) and compliance with this Order;

iii. Require the Board to maintain a Reasonable Security audit program overseen directly by the Board or a designated committee of the Board;

iv. Require the CISO to report directly to the Board in order to provide the Board with written, reliable and objective information regarding the operational effectiveness of the ISP, whether any updates or changes are recommended based on the findings from the audits, and the overall state of the ISP including how any significant risks are being addressed within the company;

v. Require ACI to maintain at all times a comprehensive mandatory training program to ensure that all relevant staff and Service Providers maintain Reasonable Security;

vi. Require the implementation or maintenance of internal controls (and the enforcement of such internal controls) to ensure that any duplicate or otherwise erroneous ACH Entries can be detected to confirm their authenticity prior to transmission into the ACH Network or other means of fund transmission;

vii. Require the use of Synthetic Data when testing or developing ACI software or systems used in connection with any consumer

financial product or service consistent with the terms of this Consent Order; and

viii. Contain specific timeframes and deadlines for implementation of the steps described above.

64. 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 in a manner that is consistent with Reasonable Security. 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 25 days.

65. 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.

VIII.

Role of the Board and Executives

IT IS FURTHER ORDERED that:

66. Respondent's Board, President and CISO (collectively Respondent's Executives) must review all plans, reports, and submissions (including the Compliance Plan, Compliance Reports, plans, reports, programs, policies,

and procedures) required by this Consent Order prior to submission to the Bureau.

67. Although this Consent Order requires Respondent to submit certain documents for review or non-objection by the Enforcement Director, Respondent's Board will have the ultimate responsibility for proper and sound management of ACI and for ensuring that ACI complies with the laws that the Bureau enforces, including Federal consumer financial laws, this Consent Order, and the Compliance Plan.

68. One year after the Effective Date, and yearly thereafter for the duration of this Order, Respondent must submit to the Enforcement Director an accurate written compliance progress report (Compliance Report) that has been approved by the Board, sworn to under penalty of perjury by each Executive, which, at a minimum:

a. Describes the steps that Respondent's Executives have taken to reasonably assess whether Respondent is complying with each applicable paragraph and subparagraph of the Consent Order and Compliance Plan;

b. Describes in reasonable detail whether and how Respondent is complying with each applicable paragraph and subparagraph of the Order, and Compliance Plan, including the manner of verification of such

compliance and any corrective actions taken to remedy potential non-compliance with the paragraph or subparagraph; and

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

69. Respondent's Executives must:

a. Authorize whatever actions are necessary for Respondent to assess whether ACI is complying with each applicable paragraph and subparagraph of the Consent Order and Compliance Plan;

b. Authorize whatever actions, including corrective actions, are necessary for Respondent to fully comply with the Consent Order; and

c. Require timely reporting by management to Respondent's Executives on the status of compliance obligations.

MONETARY PROVISIONS

IX.

Order to Pay Civil Money Penalty

IT IS FURTHER ORDERED that:

70. Under § 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, Respondent must pay a civil money penalty of $25,000,000 to the Bureau.

71. Within 20 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.

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

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

74. To preserve the deterrent effect of the civil money penalty in any Related Consumer Action, Respondent may not argue that Respondent is entitled to, nor may Respondent benefit by, any offset or reduction of any compensatory monetary remedies imposed in the Related Consumer Action because of the civil money penalty paid in this action or because of any payment that the Bureau makes from the Civil Penalty Fund. If the court in any Related Consumer Action offsets or otherwise reduces the amount of compensatory monetary remedies imposed against Respondent based on the civil money penalty paid in this action or based on any payment that the Bureau makes from the Civil Penalty Fund, Respondent must, within 30 days after entry of a final order granting such offset or reduction, notify the Bureau, and pay the amount of the offset or reduction to the U.S. Treasury. Such a payment will not be considered an additional civil money penalty and will not change the amount of the civil money penalty imposed in this action.

XI.

Additional Monetary Provisions

IT IS FURTHER ORDERED that:

75. 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.

76. 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.

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

78. 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 are required to pay to consumers and describe the consumers or classes of consumers to whom that redress has been or will be paid.

COMPLIANCE PROVISIONS

XII.

Reporting Requirements

IT IS FURTHER ORDERED that:

79. 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.

80. Within 7 days of the Effective Date, Respondent must:

a. designate at least one telephone number and email, physical, and postal addresses as points of contact that the Bureau may use to communicate with Respondent;

b. identify all businesses offering or providing a consumer financial product or service for which Respondent is the majority owner, or that

Respondent directly or indirectly controls, by all of their names, telephone numbers, and physical, postal, email, and Internet addresses; and

c. describe the activities of each such business, including the products and services offered, and the means of advertising, marketing, and sales.

81. Respondent must report any change in the information required to be submitted under Paragraph 80 at least 30 days before the change or as soon as practicable after the learning about the change, whichever is sooner, for the duration of this Order.

XIII.

Order Distribution and Acknowledgment

IT IS FURTHER ORDERED that:

82. Within 7 days of the Effective Date, Respondent must submit to the Enforcement Director an acknowledgment of receipt of this Consent Order, sworn under penalty of perjury.

83. Within 30 days of the Effective Date, Respondent must deliver a copy of this Consent Order to each Board member and executive officer, as well as to any managers, employees, or Service Providers, who have responsibilities related to the subject matter of this Consent Order.

84. 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 XII, any future Board members and executive officers before they assume their responsibilities.

85. Respondent must secure a signed and dated statement acknowledging receipt of a copy of this Consent Order within 45 days of delivery, from all persons receiving a copy of this Consent Order under this Section.

86. Ninety days from the Effective Date, Respondent must submit to the Bureau a list of all persons and their titles to whom this Consent Order has been delivered under the Section of this Order titled "Order Distribution and Acknowledgement" and a copy of all signed and dated statements acknowledging receipt of this Consent Order under Paragraph 85.

XIV.

Recordkeeping

IT IS FURTHER ORDERED that:

87. Respondent must create and retain the following business records for a period of at least 6 years from the Effective Date:

a. all documents and records necessary to demonstrate full compliance with each provision of this Consent Order, including all submissions to the Bureau;

b. for ACI's consumer bill payment service, accounting records showing the gross and net revenues generated by the service;

c. all consumer complaints and refund requests (whether received directly or indirectly, such as through a third party), and any responses to those complaints or requests;

d. records showing, for each employee providing services related to ACI's consumer bill payment service, 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; and

e. records showing, for each Service Provider providing services related to ACI's consumer bill payment service, the name of a point of contact for the person, 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 of the Service Provider.

88. Respondent must make the documents identified in Paragraph 87 available to the Bureau upon the Bureau's request.

XV.

Notices

IT IS FURTHER ORDERED that:

89. 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* ACI Worldwide Corp. et al., File No. 2023-CFPB-0005," and send them by overnight courier or 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

XVI.

Cooperation with the Bureau

IT IS FURTHER ORDERED that:

90. Respondent must cooperate to help the Bureau determine the identity and location of each Affected Consumer. Respondent must provide such information in its or its agents' possession or control within 21 days of receiving a written request from the Bureau.

91. Respondent must cooperate with the Bureau in this matter and in any investigation related to or associated with the conduct described in Section IV. Respondent must provide truthful and complete information, evidence, and testimony. Respondent must cause Respondent's officers, employees,

representatives, or agents under Respondent's control to appear for interviews, discovery, hearings, trials, and any other proceedings that the Bureau may reasonably request upon 21 days written notice, or other reasonable notice, at such places and times as the Bureau may designate, without the service of compulsory process.

XVII.

Compliance Monitoring

IT IS FURTHER ORDERED that:

92. Within 20 days of receipt of a written request from the Bureau, Respondent must submit additional Compliance Reports or other requested information related to the subject matter of this Order, which must be made under penalty of perjury; provide sworn testimony; or produce documents.

93. Respondent must permit Bureau representatives to interview any employee or other person affiliated with Respondent who has agreed to such an interview regarding: (a) this matter; (b) anything related to or associated with the conduct described in Section IV; or (c) compliance with the Consent Order. The person interviewed may have counsel present.

94. 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.

XVIII.

Modifications to Non-Material Requirements

IT IS FURTHER ORDERED that:

95. 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.

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

ADMINISTRATIVE PROVISIONS

XIX.

IT IS FURTHER ORDERED that:

97. The provisions of this Consent Order do not bar, estop, or otherwise prevent the Bureau from taking any other action against Respondent,

except as described in Paragraph 98. Further, for the avoidance of doubt, the provisions of this Consent Order do not bar, estop, or otherwise prevent any other person or governmental agency from taking any action against Respondent.

98. 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 and their 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.

99. This Consent Order is intended to be, and will be construed as, a final Consent Order issued under § 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.

100. This Consent Order will terminate on the later of 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 initiated within 5 years of the Effective Date. 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 until such time, except to the extent that any provisions of this Consent Order have been amended, suspended, waived, or terminated in writing by the Bureau or its designated agent.

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

102. Should Respondent seek to transfer or assign all or part of their 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.

103. 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 §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.

104. 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.

105. 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 26th day of June, 2023.

Rohit Chopra

Rohit Chopra
Director
Consumer Financial Protection Bureau