

Zane L. Christensen (USB 14614)
Steven A. Christensen (USB 5190)
Christensen Young & Associates, PLLC
9980 South 300 West #200
Sandy, UT 84070
Telephone: (801) 676-6447
Facsimile: (888) 569-2786

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH, CENTRAL DIVISION

Lawrence J. Mitchell, Kay Mitchell,
Matthew C. Bishop, *et al. and unknown*
Plaintiffs 1-1,000,000,

Plaintiff's,

v.

Wells Fargo Bank, National Association,
a National Banking Association, and
Wells Fargo & Company, a Delaware
Corporation, and Does, 1-5,300

Defendants.

CLASS ACTION COMPLAINT FOR:

1. Violation of Utah Unfair Competition Act,
Utah Code Annotated 13-5a-101 et seq.;
2. Invasion of Privacy - Intrusion, Public
Disclosure of Private Facts,
Misappropriation of Likeness and
Identity, and Utah Constitutional Right to
Privacy;
3. Negligence;
4. Breach of Contract and Bailment;
5. Conversion;
6. Fraud and other actions set forth herein

Judge: **Clark Waddoups**

Case:2:16-cv-00966 - CW

Demand for Jury Trial

COME NOW Plaintiffs Lawrence J. Mitchell, Kay Mitchell, and Matthew C. Bishop, individually and on behalf of all unknown Plaintiffs, 1-1,000,000 ("Plaintiffs") and bring this class action against Defendants Wells Fargo Bank, National Association and Wells Fargo & Company (collectively "Wells Fargo") a Delaware corporation, and DOES 1-5,300 (collectively, "Defendants") on behalf of themselves and all others similarly situated to obtain damages, restitution and injunctive relief for the Class, as defined, below, from Defendants. Plaintiffs make the following allegations upon information and belief, except as to their own actions, the investigation of their counsel, and the facts that are a matter of public record, and aver and allege

as follows:

1. Plaintiff Lawrence J. Mitchell and Kay Mitchell are residents of South Jordan, County of Salt Lake, Utah.
2. Plaintiff Matthew is a resident of Salt Lake County, State of Utah.
3. Defendant Wells Fargo & Company is, and at all times relevant hereto was, a corporation organized and existing under the laws of the State of Delaware. Wells Fargo & Company is a financial services company with over \$1.5 trillion in assets, and provides banking, insurance, investments, mortgage, and consumer and commercial finance through more than 9,000 locations, 12,000 ATMs, and via Internet. It has approximately 265,000 full-time employees, and is ranked 29th on Fortune Magazine's 2014 rankings of America's 500 largest corporations.
4. Defendant Wells Fargo Bank, National Association is, and at all times relevant hereto was, a national banking association chartered under the laws of the United States, with its primary place of business in Sioux Falls, South Dakota. Wells Fargo Bank, National Association provides Wells Fargo & Company's personal and commercial banking services, and is Wells Fargo & Company's principal subsidiary.
5. The true names and capacities of Defendants sued herein as DOES 1 through 5,300, inclusive, are unknown to the People, who therefore sue said Defendants by such fictitious
6. Wells Fargo boasts about the average number of products held by its customers, currently approximately six bank accounts or financial products per customer. Wells Fargo seeks to increase this to an average of eight bank accounts or financial products per account holder, a company goal Wells Fargo calls the "gr-eight" initiative.
7. Wells Fargo's resulting market dominance has come at a significant price to the general public, because it has been achieved in large part through an ambitious and strictly enforced sales quota system. Wells Fargo quotas are difficult for many bankers to meet without resorting to the abusive and fraudulent tactics described further below. Moreover, Wells Fargo enforces its sales quotas by constant monitoring. Daily sales for each branch, and each sales employee, are reported and discussed by Wells Fargo's District Managers four times a day, at 11:00 a.m., 1:00 p.m., 3:00p.m., and 5:00p.m. Those failing to meet daily sales quotas are approached by management, and often reprimanded and/or told to "do whatever it takes" to meet their individual

sales quotas.

8. Consequently, Wells Fargo's managers and bankers have for years engaged in unethical, and illegal practices called "gaming." Gaming consists of, among other things, opening and manipulating fee generating customer accounts through often unfair, fraudulent, and unlawful means, such as omitting signatures and adding unwanted secondary accounts to primary accounts without permission. Other practices utilized as part of these "gaming" schemes have included misrepresenting the costs, benefits, fees, and/or attendant services that come with an account or product, all in order to meet sales quotas.

9. At all relevant times, each Defendant was acting as an agent, servant, assignee, representative, partner, joint venturer, co-conspirator, or employee of the other Defendants, and, in doing the acts alleged herein, were actions within the course and scope of said agency, service, assignment, representation, partnership, joint venture, conspiracy, or employment. Due to the relationship between Defendants, each Defendant has knowledge or constructive notice of the acts of each of the other Defendants.

10. Each Defendant is a "person" within the meaning of Utah Statutes.

11. In this Complaint, when reference is made to any act or omission of a Defendant, such allegations shall include the acts, and omissions of owners, officers, directors, agents, employees, contractors, vendors, affiliates, and representatives of said Defendant while acting within the course and scope of their employment or agency on behalf of said Defendant.

JURISDICTION AND VENUE

12. This Court has original jurisdiction pursuant to 28 U.S.C. §1332(d)(2). In the aggregate, Plaintiffs claims and the claims of the other members of the Class exceed \$5,000,000.00 exclusive of interest and costs, and there are numerous class members who are citizens of states other than Wells Fargo's state of citizenship.

13. This Court has personal jurisdiction over Wells Fargo because Wells Fargo is authorized to do business in the State of Utah, and operates stores within this Judicial District and Wells Fargo has significant continuous and pervasive contacts with the State of Utah, and maintains numerous banking establishments and employees in the State of Utah, including, upon

information and belief, some of the 5,300 employees who were terminated by Wells Fargo for engaging in the gaming tactic established by Wells Fargo.

14. This Court has personal jurisdiction over Plaintiffs because they are residents of the State of Utah.

15. Venue is proper in this Court pursuant to 28 U.S.C. §1391 because a substantial part of the events and/or omissions giving rise to the Plaintiffs claims and Class Member claims arise in this action or occurred in this District and because Defendants are subject to personal jurisdiction in this District.

GENERAL ALLEGATIONS

16. Upon information and belief, Wells Fargo is within the top thirty (30) of America's largest corporations, ranked 29th on the Fortune 500 list of top American companies.

17. Wells Fargo's *modus operandi* is to attempt to get each customer to maintain numerous accounts with Wells Fargo. In, a brochure published by Wells Fargo called "The Vision & Values: of Wells Fargo;" Wells Fargo' states: "Going for gr-eight,' Our average retail banking household has about six products with us. We want to get to eight... and beyond. One of every four already has eight or more. Four of every 10 have six or more."

18. In its 2014 Annual Report to the U.S: Securities and Exchange Commission, Wells Fargo boasts about its "products" 'per customer and its "cross-sell strategy," "Our vision is to satisfy all our customers' financial needs, help them succeed financially, be recognized as the premier financial services company in our markets and be one of America's great companies. Important to our strategy to achieve this vision is to increase the number of our products our customers use and to offer them all of the financial products that fulfill their financial needs." That report further states: "Our cross-sell strategy is to increase the number of products our customers use by offering them all of the financial products that satisfy their financial needs."

19. Wells Fargo further stated in its 2014 Annual Report to the U.S. Securities & Exchange Commission: "we continued to maintain our solid customer relationships across the Company, with retail banking household cross-sell of 6.17 products per household (November 2014); Wholesale Banking cross-sell of 7.2 products per relationship (September 2014); and Wealth, Brokerage and Retirement cross-sell of 10.49 products per retail banking household

(November 2014)." Wells Fargo further stated in that same filing: "We believe there is more opportunity for cross-sell as we continue to earn more business from our customers. Our goal is eight products per household"

20. In order to achieve its goal of eight accounts per household, Wells Fargo imposes unrelenting pressure on its bankers to open numerous accounts per customer.

21. Wells Fargo has strict quotas regulating the number of daily "solutions" that its bankers must reach; these "solutions" include the opening of all new banking and credit card accounts. Managers constantly hound, berate, demean and threaten employees to meet these unreachable quotas. Managers often tell employees to do whatever it takes to reach their quotas. Employees who do not reach their quotas are often required to work hours beyond their typical work schedule without being compensated for that extra work time, and/or are threatened with termination.

22. The quotas imposed by Wells Fargo on its employees are often not attainable because there simply are not enough customers who enter a branch on a daily basis for employees to meet their, quotas through traditional means.

23. Wells Fargo's bankers are thus naturally and predictably forced to resort to alternative means to meet quotas, including using high pressure sales tactics to coerce customers into opening additional accounts or using inaccurate or misleading information about potential accounts to induce customers to open them.

24. Wells Fargo employees also pressure their own family members and friends to sign up for accounts to meet their quotas. Some employees report that they have "tapped out" every family member and friend for accounts. Others report that they spend holiday dinners trying to convince family members to sign up for accounts. Management encourages employees to achieve "solutions" through family members. Since these accounts are opened by friends and family as favors, they are often unfunded, and can result in fees charged by Wells Fargo to its own employees' families or acquaintances, even for such "zero balance" accounts.

25. Employees thus resort to *gaming tactics* to increase their "solutions," and meet minimum quotas. Gaming is so ingrained in the business of Wells Fargo that many of the tactics, employed to meet these sky-high quotas have commonly-used names.

These gaming practices are so pervasive within Wells Fargo's business model that some methods of gaming have even been given their own names.

a. *"Sandbagging"* refers to Wells Fargo's practice of failing to open accounts when requested by customers, and instead accumulating a number of account applications to be opened at a later date. Specifically, Wells Fargo employees collect manual applications for various products, stockpile them in an unsecured fashion, and belatedly open up the accounts (often with additional, unauthorized accounts) in the next sales reporting period, frequently before or after banking hours, or on bank holidays such as New Year's Day.

b. *"Pinning"* refers to Wells Fargo's practice of assigning, without customer authorization, Personal Identification Numbers ("PINs") to customer ATM card numbers with the intention of, among other things, impersonating customers on Wells Fargo computers, and enrolling those customers in online banking and online bill paying without their consent.

c. *"Bundling"* refers to Wells Fargo's practice of incorrectly informing customers that certain products are available only in packages with other products such as additional accounts, insurance, annuities, and retirement plans.

26. While Wells Fargo has recently terminated over 5,300 employees (by all sources is but a fraction of employees who participated in these illegal activities) who engaged in these types of illegal, unethical behavior, they still reward individuals such as Carrie Tolstedt, who was the Wells Fargo executive overseeing much of this behavior, and who was referred to as the "chief sandbagger," with over a \$124 million dollar termination payment.

27. Upon information and belief Carrie Tolstedt was the Wells Fargo executive who was in charge of the unit where employees opened more than 2 million unauthorized customer accounts. Wells Fargo continues to encourage this illegal conduct which they acknowledge is unfair and abusive practices under federal law. Wells Fargo is in violation of trust and an abuse of trust, then they pay off the scape goat with millions of dollars, as Wells Fargo abuses government programs that were intended to assist and help people after the financial meltdown.

28. Last year, while engaging in employee abuse, and customer fraudulent practices, Tolstedt continued to push "strong cross-selling ratios". In fact Wells Fargo has singled out Tolstedt and other executives touting the bank's "expertise" in selling multiple products which was immensely profitable for the bank.

29. Even after determining that the problems existed, years ago, Wells Fargo took no action to terminate the fraudulent activities, they continued to promote and monetarily reward individuals who opened fraudulent accounts, fabricated false emails, PIN numbers, and intentionally sold customers bundled accounts they did not need or desire.

30. Upon information and belief, Wells Fargo employees opened over 1,534,280 deposit accounts that may not have been authorized and that may have been funded through simulated funding, or transferring funds from consumers' existing accounts without their knowledge or consent.

31. That analysis determined that roughly 85,000 of those accounts incurred about \$2 million in fees. The fees included overdraft fees on linked accounts the consumers already had, monthly service fees imposed for failure to keep a minimum balance in the unauthorized account, and other fees.

32. Section 1036(a)(1)(B) of the CFPA prohibits "unfair" acts or practices. 12 U.S.C. § 5536(a)(1)(B). An act or practice is unfair if it causes or is likely to cause consumers substantial injury that is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or to competition. 12 U.S.C. § 5531(c)(1).

33. By opening unauthorized deposit accounts and engaging in acts of simulated funding, Wells Fargo caused and was likely to cause substantial injury to consumers that was not reasonably avoidable, because it occurred without consumers' knowledge, and was not outweighed by countervailing benefits to consumers or to competition.

34. Section 1036(a)(1)(B) of the CFPA prohibits "abusive" acts or practices. 12 U.S.C. § 5536(a)(1)(B). An act or practice is abusive if it materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service. 12 U.S.C. § 5531(d)(1). Additionally, an act or practice is abusive if it takes unreasonable advantage of the inability of the consumer to protect his or her interests in selecting or using a consumer financial product or service. 12 U.S.C. § 5531(d)(2)(B).

35. Wells Fargo's acts of opening unauthorized deposit accounts and engaging in simulated funding materially interfered with the ability of consumers to understand a term or condition of a consumer financial product or service, as they had no or limited knowledge of those terms and conditions, including associated fees.

36. Additionally, Wells Fargo's acts of opening unauthorized deposit accounts and engaging in simulated funding took unreasonable advantage of consumers' inability to protect their interests in selecting or using consumer financial products or services, including interests in having an account opened only after affirmative agreement, protecting themselves from security and other risks, and avoiding associated fees.

37. Therefore, Respondent engaged in “unfair” and “abusive” acts or practices that violate §§ 1031(c)(1), (d)(1), (d)(2)(B), and 1036(a)(1)(B) of the CFPA. 12 U.S.C. §§ 5531(c)(1), (d)(1), (d)(2)(B), 5536(a)(1)(B).

38. Wells Fargo’s analysis concluded that its employees submitted applications for 565,443 credit-card accounts that may not have been authorized by using consumers’ information without their knowledge or consent. That analysis determined that roughly 14,000 of those accounts incurred \$403,145 in fees. Fees incurred by consumers on such accounts included annual fees and overdraft-protection fees, as well as associated finance or interest charges and other late fees.

39. Section 1036(a)(1)(B) of the CFPA prohibits “unfair” acts or practices. 12 U.S.C. § 5536(a)(1)(B). An act or practice is unfair if it causes or is likely to cause consumers substantial injury that is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or to competition. 12 U.S.C. § 5531(c)(1).

40. By applying for and opening credit-card accounts using consumers’ information without their knowledge or consent, Wells Fargo caused and was likely to cause substantial injury that was not reasonably avoidable, because it occurred without consumers’ knowledge, and was not outweighed by countervailing benefits to consumers or competition.

41. Section 1036(a)(1)(B) of the CFPA prohibits “abusive” acts or practices. 12 U.S.C. § 5536(a)(1)(B). An act or practice is abusive if it materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service. 12 U.S.C. § 5531(d)(1). Additionally, an act or practice is abusive if it takes unreasonable advantage of the consumer’s inability to protect his or her interests in selecting or using a consumer financial product or service. 12 U.S.C. § 5531(d)(2)(B).

42. Wells Fargo’s acts of opening credit-card accounts using consumers’ information without their knowledge or consent materially interfered with the ability of consumers to understand a term or condition of a consumer financial product or service, as they had no or limited knowledge of those terms and conditions, including associated fees.

43. Additionally, Wells Fargo’s acts of opening credit-card accounts using consumers’ information without their knowledge or consent took unreasonable advantage of the consumers’ inability to protect their interests in selecting or using a consumer financial product or service.

44. Therefore, Wells Fargo engaged in “unfair” and “abusive” acts or practices that violate §§ 1031(c)(1), (d)(1), (d)(2)(B), and 1036(a)(1)(B) of the CFPA. 12 U.S.C. §§ 5531(c)(1), (d)(1), (d)(2)(B), 5536(a)(1)(B).

45. During the Relevant Period, Wells Fargo’s employees used email addresses not belonging to consumers to enroll consumers in online-banking services without their knowledge or consent. Section 1036(a)(1)(B) of the CFPA prohibits “abusive” acts or practices. 12 U.S.C. § 5536(a)(1)(B). An act or practice is abusive if it takes unreasonable advantage of the consumer’s inability to protect his or her interests in selecting or using a consumer financial product or service. 12 U.S.C. § 5531(d)(2)(B).

46. Wells Fargo’s acts of enrolling consumers in online-banking services without their knowledge or consent took unreasonable advantage of consumers’ inability to protect their interests in selecting or using a consumer financial product or service, including interests in having these products or services activated only after affirmative agreement and protecting themselves from security and other risks.

47. Therefore, Wells Fargo engaged in “abusive” acts or practices that violate §§ 1031(d)(2)(B) and 1036(a)(1)(B) of the CFPA. 12 U.S.C. §§ 5531(d)(2)(B), 5536(a)(1)(B).

48. During the relevant period, Wells Fargo’s employees requested debit cards and created PINs to activate them without consumers’ knowledge or consent. 35. Section 1036(a)(1)(B) of the CFPA prohibits “abusive” acts or practices. 12 U.S.C. § 5536(a)(1)(B). An act or practice is abusive if it takes unreasonable advantage of the consumer’s inability to protect his or her interests in selecting or using a consumer financial product or service. 12 U.S.C. § 5531(d)(2)(B).

49. Wells Fargo’s acts of issuing debit cards to consumers without their knowledge or consent took unreasonable advantage of consumers’ inability to protect their interests in selecting or using a consumer financial product or service. 12 U.S.C. § 5531(d)(2)(B)..

50. Therefore, Wells Fargo engaged in “abusive” acts that violate §§ 1031(d)(2)(B) and 1036(a)(1)(B) of the CFPA. 12 U.S.C. §§ 5531(d)(2)(B), 5536(a)(1)(B)

51. Wells Fargo has strict quotas regulating the number of daily "solutions" that its bankers must reach; these "solutions" include the opening of all new banking and credit card accounts. Managers constantly hound, berate, demean and threaten employees to meet these unreachable quotas. Managers often tell employees to do whatever it takes to reach their quotas.

52. Employees who do not reach their quotas are often required to work hours beyond their typical work schedule without being compensated for that extra work time, and/or are threatened with termination.

53. Customers who complain about receiving credit cards they did not request are advised by Wells Fargo to simply destroy the unrequested and unauthorized cards: However; simply destroying these unauthorized cards does not close the account nor repair the impact to a customer's credit profile.

54. In the practice known at Wells Fargo as "pinning," a Wells Fargo banker obtains a debit card number, and personally sets the PIN, often to 0000, without customer authorization.

"Pinning" permits a banker to enroll a customer in online banking, for which the banker would receive a solution (sales credit). To bypass computer prompts requiring customer contact information, bankers impersonate the customer online, and input false generic email addresses such as 1234@wellsfargo.com, noname@wellsfargo.com, or none@wellsfargo.com to ensure that the transaction is completed, and that the customer remains unaware of the unauthorized activity.

55. Because of Wells Fargo's on-going setting of unrealistic sales goals, Wells Fargo employees have engaged in, and continue to engage in, other gaming tactics, including, but not limited to:

- a. Making misrepresentations to customers to get them to open additional accounts such as falsely stating: "you will incur a monthly fee on your checking account until you add a savings account."
- b. Misrepresenting that additional accounts do not have monthly fees, when they actually do incur such fees.
- c. Referring unauthorized, and therefore unfunded, accounts to collections because, Wells Fargo's practices, cause the accounts to have negative balances.
- d. Wells Fargo sold heavy to individuals holding Mexican Matriculada Consular cards because the lack of a Social Security Number makes it easier to open numerous fraudulent accounts.
- e. Advising customers who do not want credit cards that they will be sent a credit card anyway, and to just tear it up when they receive it.

56. Customers who have discovered unauthorized accounts often make the discovery accidentally. For instance: (a) unexplained money being withdrawn from authorized accounts to fund unauthorized accounts; (b) mailings from Wells Fargo congratulating a customer on opening a new account the customer does not recognize, or asking a customer to update account information for accounts that the customer does not recognize; (c) calls from collection agencies

stating the customer is overdrawn on an account that the customer does not recognize; and (d) discovering that checks a customer intended to be deposited into an authorized account do not appear in monthly statements because the checks had instead been deposited into an unauthorized account.

57. Customers have been prejudiced in numerous ways by Wells Fargo's gaming: (a) customers lose money to monthly service fees charged for unauthorized accounts; (b) customer accounts are placed into collection, forcing customers to fight with debt collection agencies for fees charged by Wells Fargo on unauthorized accounts; (c) customers' credit reports are impacting job applications, loans for automobiles, and mortgage applications; and (d) customers are forced to purchase costly identity theft protection services to ensure against further activities. But for Wells Fargo's quota-based business model, its customers would not have incurred wrongful fees, been put into collections, suffered derogatory references on their credit reports, or forced to purchase identity theft protection.

58. Customers' unauthorized accounts remain open, despite repeated customer requests to Wells Fargo to close those accounts.

59. Customers have difficulty reporting unauthorized activity. Reaching the correct representative is no guarantee the unauthorized account will be remedied, as complaining customers often never receive return calls from Wells Fargo.

60. Wells Fargo knew, or in the exercise of reasonable care should have known, that its employees would not report the complaint, because upon information and belief, Wells Fargo executives, such as Carrie Tolstedt were more concerned with profit and the “**gr-eight**” program.

61. Wells Fargo requires that all new customer accounts be approved by a branch manager or assistant manager, thereby providing Wells Fargo management with a clear record of the number and types of accounts opened for each customer.

62. Despite Wells Fargo's knowledge of gaming by its employees, it has done little, if anything, to terminate these practices, nor to reform the business model it created that has fostered them. While Wells Fargo has made a few minor changes to its policies, and has terminated a handful of employees, those efforts have been, at most, cosmetic, and ultimately benefit Wells Fargo by providing them with plausible deniability. However, the policies that encourage these tactics continue, and employees who engage in them continue to be rewarded monetarily, and even promoted, as Plaintiffs believe was the situation with Carrie Tolstedt.

Wells Fargo has not altered its quota system, nor has it reduced the illegal fraudulent activities, identity theft, manipulation of processing customer debit card purchases to maximize overdraft fees, et. al.

63. Wells Fargo has a plethora of fines, refusal to follow regulatory Orders, DOJ settlement agreements, because the United States Government decided it is “to big to fail” it can do what ever it wants and uses interest free money from the United States and the customers to pay judgments because they make so much money, it doesn’t really effect their role in the US.

CLASS ACTION ALLEGATIONS

64. Plaintiffs bring this action on their own behalf, and on behalf of all other persons similarly situated ("the Class"). The Class that Plaintiffs seek to represent is:

A. All persons who had checking, savings, brokerage accounts, financial advisors, mortgages, or used any of Wells Fargo’s banking services beginning on a date unknown to Plaintiffs, but within the four years preceding the filing of this Complaint. Excluded from the Class are Defendants; officers, directors, and employees of Defendants; any entity in which Defendants have a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of the Defendants.

B. All persons who purchased services from Wells Fargo not during the affected time period, but whose identifying information was stored on Wells Fargo’s database. Excluded from the Class are Defendants; officers, directors, and employees of Defendants; any entity in which Defendants have a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of the Defendants.

C. All persons who have been financially harmed or damaged because of Wells Fargo’s fraudulent conduct, had improper fees accessed against their accounts, improper overcharges, had their accounts bundled, were sandbagged, or victims of pinning, subjected to financial harm or damages, loss of time, bank charges, late fees, and/or other miscellaneous costs and damages. Excluded from the Class are Defendants; officers, directors, and employees of Defendants; any entity in which Defendants have a controlling interest; the affiliates, legal representatives, attorneys, heirs, and assigns of these Defendants.

65. The members of the Class are so numerous that the joinder of all members is impractical. While the exact number of Class members is unknown to Plaintiffs at this time, based on information and belief, it is in the hundreds of thousands.

66. There is a well-defined community of interest among the members of the Class because common questions of law and fact predominate, Plaintiffs claims are typical of the members of the Class, and Plaintiffs can fairly and adequately represent the interests of the Class.

67. This action satisfies the requirements of Federal Rules of Civil Procedure, Rule 23(b)(3) because it involves questions of law and fact common to the members of the Class that predominate over any questions affecting only individual members, including, but not limited to:

- a. Whether Defendants, jointly and severally, unlawfully used, maintained, lost or disclosed Class members' personal and/or financial information;
- b. Whether Wells Fargo created a hostile working environment which fostered and rewarded fraudulent actions by its employees.
- c. Whether all Defendants violated the requirements of Utah Code Annotated, Section 13-5a 103 *et seq.*
- d. Whether all Defendants' conduct was negligent, and/or grossly negligent;
- e. Whether all Defendants acted willfully and/or with oppression, fraud, malice, or indifference to the consequences to Plaintiffs;
- f. Whether all Defendants' conduct constituted intrusion;
- g. Whether Defendants' conduct constituted public disclosure of private facts;
- h. Whether all Defendants' conduct constituted misappropriation of likeness and identity;
- i. Whether all Defendants' conduct violated Class members' Utah Constitutional Right to Privacy;
- j. Whether all Defendants' conduct constituted bailment and breach of contract;
- k. Whether all Defendants' conduct constituted conversion;
- l. Whether Plaintiffs and the Class are entitled to damages, civil penalties, punitive damages, and/or injunctive relief;
- n. Whether Plaintiffs and Class Members are entitled to declaratory and injunctive relief;
- o. Whether Wells Fargo Management engaged in theft of customers funds;

68. Plaintiffs claims are typical of those other Class members who have likewise been subjected to financial harm or damages, loss of time, bank charges, late fees and/or other miscellaneous costs and damages.

69. Plaintiffs will fairly and accurately represent the interests of the Class.

70. The prosecution of separate actions by individual members of the Class would create a

risk of inconsistent or varying adjudications with respect to individual members of the Class, which would establish incompatible standards of conduct for Defendants and would lead to repetitive adjudication of common questions of law and fact. Accordingly, class treatment is superior to any other method for adjudicating the controversy. Plaintiffs know of no difficulty that will be encountered in the management of this litigation that would preclude its maintenance as a class action under Rule 23(b)(3).

71. Damages for any individual class member are likely insufficient to justify the cost of individual litigation, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go un-remedied without certification of the Class.

72. Defendants have acted or refused to act on grounds that apply generally to the class, as alleged above, and certification is proper under Rule 23(b)(2).

FIRST CLAIM FOR RELIEF

73. Plaintiffs incorporate by reference paragraphs 1-72 as if fully set forth fully herein.

74. Defendants' conduct constitutes unfair and illegal and fraudulent business practices within the meaning of the Utah Unfair Competition Law.

75. Defendants' conduct violated certain laws as alleged herein, and, *ergo*, by engaging in the said conduct in the course of doing business, Defendants engaged in unlawful business practices in violation of the Utah Unfair Competition Law, Utah Code Annotated (UCA) § 13-5a-101 *et seq.*

76. Plaintiffs contend that by engaging in the above-described conduct in the course of doing business, Defendants engaged in unfair business practices in violation of the Utah Unfair Competition Law (U.C.A. § 13-5a-101 *et seq.*). The harm and potential harm to each Plaintiff outweighed any utility that Defendants' conduct may have produced.

77. Wells Fargo aggravated the damage to consumers from their employees actions of manipulating account information, fabricating emails allegedly belonging to customers,

making illegal data entries, engaging in fraudulent activity on the customers accounts. Wells Fargo was aware of the ongoing breaches and failed to provide adequate and prompt notice. Consumers were and are entitled to adequate and prompt notification about the illegal actions to help them mitigate the harm and avoid additional instances of fraud as alleged herein. Wells Fargo, however, failed to take reasonable steps to notify consumers that their information has been compromised.

78. Beginning on a date unknown to the Plaintiffs, but within the four years preceding the filing of this Complaint, Defendants and Does 1-100, and each of them, have violated and conspired to violate the UCL by engaging in one or more of the following *unlawful* business acts and practices, among others:

- a. Willfully obtaining personal identifying information of another person (which includes name, address, telephone number, health insurance number, taxpayer identification number, school identification number, state or federal driver's license or identification number, Social Security number, place of employment, employee identification number, professional or occupational number, mother's maiden name, demand deposit account number, savings account number, checking account number, PIN or password, alien registration number, government passport number, and date of birth), and using that information for an unlawful purpose, including to obtain or attempt to obtain credit, goods, services, real property, or medical information without the consent of that person.
- b. Being a party to any fraudulent conveyance of any contract or conveyance had, made, or, contrived, with intent to deceive and defraud others, or while being a, parry to any fraudulent conveyance of any contract or conveyance, wittingly and willingly putting in, using, avowing, maintaining, justifying, or defending the fraudulent conveyance of any contract or conveyance as true and done, had or made in good faith, or upon good consideration.
- c. Knowingly accessing and without permission using data, computers, computer systems, or computer networks to execute a scheme to defraud or wrongfully obtain money, property, or data.
- d. Knowingly accessing, and without permission taking, copying, or making use of customer information, in violation of Utah's Unfair Competition Law.
- e. Knowingly accessing, and without permission taking, copying, or making use of, customer information, in violation of 15 United States Code Section 680, *et seq.*, and the rules and regulations promulgated thereunder.

79. Beginning on a date unknown to the People, but within the four years preceding the filing of this Complaint, Defendants and Does 1-5,300, and each of them, have violated and

conspired to violating the UCL by engaging in one or more of the following unfair business acts and practices, among others:

- a. Threatening incipient violations of the aforementioned Utah laws; and violated the public policy embodied in and the spirit of those laws;
- b. Violation of the established public policy of the State of Utah, which among other things, seeks to ensure that: all monetary contracts are duly authorized by each party; all bank accounts are authorized and agreed to by the customer in whose name the bank account is opened; residents of the state are not harmed in their credit reports by acts not actually performed, or debts not actually incurred, by that resident; personal information of an individual is not improperly obtained and used for, an unlawful purpose; and that when, personal, information is obtained without authority;; that the person whose information .was obtained is informed immediately.
- c. Defendants' conduct as described in this Complaint has been immoral, unethical, oppressive and unscrupulous in that Defendants: (1) profited by improperly signing customers up for bank accounts to which the customers did not agree; (2) boast about the average number of accounts per customer they have achieved, knowing that many of those accounts were unauthorized; (3) expose the consumer to financial hardships involving unjustified debt collection and negative credit reporting, thus jeopardizing those customers' ability to obtain mortgages, automobile loans, and employment; and (4) otherwise garnered an unfair advantage over lawfully competing businesses.
- d. Wells Fargo's acts and practices alleged in this Complaint have had, and continue to have, a substantial detrimental impact upon its customers and the community. This detrimental impact is not outweighed by any countervailing reasons, justifications, and motives of Wells Fargo. In short, the harm experienced by the customers and the surrounding community far outweighs the utility of Wells Fargo's conduct.

80. Beginning on a date unknown to the People, but within the four years preceding the filing of this Complaint, Defendants, and each of them, have violated and conspired to violate the Utah Unfair Competition Law by engaging in one or more of the following *fraudulent* business acts and practices, among others:

- a. Using misrepresentations, deception, and concealment of material information to open unauthorized accounts in customers' names.
- b. Using misrepresentations, deception, and concealment of material information and then failing to reveal to the customers that their personal information was compromised.

SECOND CLAIM FOR RELIEF

81. Plaintiff incorporate by reference paragraphs 1-80 as if set forth in full particularity herein.

82. The Stored Communications Act ("SCA") contains provisions that provide consumers

with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, “to protect individuals’ privacy interests in personal and proprietary information.” S. Rep. No. 99-541, at 3 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555 at 3557.

83. Section 2702(a)(1) of the SCA provides that “a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.” 18 U.S.C. § 2702(a)(1).

84. The SCA defines “electronic communication service” as “any service which provides to users thereof the ability to send or receive wire or electronic communications.” *Id.* at § 2510(15).

85. Through its payment processing equipment, Wells Fargo provides an “electronic communication service to the public” within the meaning of the SCA because it provides consumers at large with credit and debit card payment processing capability that enables them to send or receive wire or electronic communications concerning their private financial information to transaction managers, card companies, or banks.

86. By failing to take commercially reasonable steps to safeguard sensitive private financial information, even after Wells Fargo was aware that customers’ private and confidential information had been compromised by its own employees, Wells Fargo has knowingly divulged customers’ private financial information that was communicated to financial institutions, while in electronic storage in Wells Fargo’s data systems.

87. Section 2702(a)(2)(A) of the SCA provides that “a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service on behalf of, and

received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service.” 18 U.S.C. § 2702(a)(2)(A).

88. The SCA defines “remote computing service” as “the provision to the public of computer storage or processing services by means of an electronic communication system.” 18 U.S.C. § 2711(2).

89. An “electronic communications systems” is defined by the SCA as “any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications.” 18 U.S.C. § 2510(4).

90. Wells Fargo provides onsite and remote computing services to its customers and the public by virtue of its computer processing services, including, but not limited to, banking services, consumer credit and debit card payments, *etc.* which are used by customers and carried out by means of an electronic communications system, namely the use of wire, electromagnetic, photo-optical or photo-electric facilities for the transmission of wire or electronic communications received from, and on behalf of, the customer concerning customer private financial information.

91. By failing to take commercially reasonable steps to safeguard sensitive private financial information, and requiring scrutiny of their own employees, Wells Fargo has knowingly divulged customers’ private financial information that was carried and maintained on Wells Fargo’s computing data bank services.

92. As a result of Wells Fargo’s conduct described herein and its violations of Sections 2702(a)(1) and (2)(A) of the SCA, Plaintiffs and Class Members have suffered actual

identity theft, as well as damages in the form of (i) improper disclosure of their private confidential information; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the Data Breach; (iii) the value of their time spent mitigating identity theft and/or identity fraud, and/or the increased risk of identity theft and/or identity fraud; (iv) and deprivation of the value of their private information, for which there is a well-established national and international market. Plaintiffs, on their own behalf and on behalf of the Class Members, seek an order awarding themselves and the Class Members the maximum statutory damages available under 18 U.S.C. § 2707, in addition to the cost for 3 years of credit monitoring services.

WHEREFORE, Plaintiffs, on their own behalf and on behalf of the Class, pray for entry of judgment jointly and severally against Defendants, and awarding Plaintiffs and the Class compensatory damages, statutory damages, treble damages, punitive damages, and reasonable attorney's fees and costs; and such other and further relief as this Court deems just and proper.

THIRD CLAIM FOR RELIEF

93. Plaintiffs incorporate by reference paragraphs 1-92 as if set forth in full particularity herein.

94. Plaintiffs, and the other Class Members, had a reasonable expectation of privacy in the private information Defendants Wells Fargo obtained from them in opening accounts. Said information was provided in a fiduciary capacity, and Wells Fargo and its employees mishandled and/or failed to protect said information, and knowingly violated their fiduciary duties.

95. By failing to keep Plaintiffs private information safe, and by misusing and/or disclosing said information to unauthorized parties for unauthorized use, Defendants invaded Plaintiffs privacy by:

- a. intruding into Plaintiffs private affairs in a manner that would be highly offensive to a reasonable person;
- b. publicizing private facts about Plaintiffs, which is highly offensive to a reasonable person;
- c. using and appropriating Plaintiffs identity without Plaintiffs' consent;
- d. violating Plaintiffs right to privacy under Utah Constitution, Article 1, Section 1, through the improper use of Plaintiff s private information properly obtained for a specific purpose for another purpose, or the disclosure of it to some third party.

96. Plaintiffs allege that Defendants knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs position would consider Defendants' actions highly offensive.

97. Plaintiffs assert that Defendants, jointly and severally invaded Plaintiffs and the Class Members right to privacy and intruded into Plaintiffs private affairs by misusing and/or disclosing Plaintiffs private information without their informed, voluntary, affirmative and clear consent, and/or failed to properly secure confidential information by encouraging employees to abuse the customers private information for purposes of promotions, personal gains, and monetary remuneration.

98. Plaintiffs allege that Wells Fargo had been aware of the employee violations for over a year before taking any action, but failed to take action in lieu of maximizing financial gains from the employees unethical behavior that Wells Fargo was fully aware of, and thereby exposed Plaintiffs to added, unnecessary risk. From 2011 the bank opened more than 2 million deposit and credit card accounts that may not have been authorized.¹

99. Plaintiffs contend that as a direct and proximate result of such misuse and disclosures, Plaintiffs reasonable expectations of privacy in their private information was unduly frustrated and thwarted, and that the Defendants' conduct amounted to a serious invasion of

¹ Wells Fargo employees pushed checking account customers into savings, credit and online accounts that could generate fees. Bank employees were told that the average customer tapped six financial tools but that they should push households to use eight products, according to the complaint. The bank opened more than 2 million deposit and credit card accounts that may not have been authorized, according to the CFPB. <http://www.cnbc.com/2016/09/08/wells-fargo-reaches-185m-settlement-to-settle-secret-account-fraud-case.html>

Plaintiffs' and the Class Members protected privacy interests.

100. Plaintiffs assert Defendants had a duty to protect Plaintiffs private information and that in failing to protect Plaintiffs private information, and in misusing and/or disclosing Plaintiffs private information, Defendants have acted with malice, oppression and in conscious disregard of Plaintiffs and the Class members' rights to have such information kept confidential and private. Plaintiffs, accordingly, seek an award of compensatory damages, nominal damages, punitive damages, attorneys' fees, expert witness fees, and associated court costs on their behalf as well as on behalf of the Class.

FOURTH CLAIM FOR RELIEF

101. Plaintiffs incorporate the allegations in paragraphs 1-100 as if set forth with full particularity herein.

102. Plaintiffs assert that under the Gramm-Leach-Bliley Act, 15 U.S.C. § 6801, Wells Fargo had a duty to protect and keep sensitive personal information that it obtained from customers that conducted banking, financial, credit card and debit card transactions, or other services, secure, private, and confidential.

103. Plaintiffs allege that Wells Fargo violated the Gramm-Leach-Bliley Act by: (a) not adequately safeguarding Plaintiffs' and the Class Members' sensitive personal information, (b) encouraging and rewarding its employees for violating privacy provisions of the Act in order to maximize financial gain; and (c) failing to follow applicable state law designed to protect cardholder information.

104. Plaintiffs contend that Wells Fargo's encouragement and reward to employees for violations of privacy provisions, and those accompanying rules and regulations, and to follow applicable state law constitutes conspiracy and negligence *per se*.

105. Plaintiffs assert that as a result of Wells Fargo's conduct alleged herein, Plaintiffs and

Class Members suffered actual identity theft, as well as damages in the form of (i) improper disclosure of their private and confidential information; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the data breach; (iii) the value of their time spent mitigating identity theft and/or identity fraud, and/or the increased risk of identity theft and/or identity fraud; (iv) and deprivation of the value of their private and confidential information, for which there is a well-established national and international market.

106. Plaintiffs assert that as a direct and proximate result of Defendant's negligence *per se* Plaintiffs and Class Members were damaged and harmed to their detriment and seek the award of actual damages, compensatory damages, attorneys' fees, and such other and further damages as this Court deems just and reasonable.

WHEREFORE, Plaintiffs, on their own behalf and on behalf of the Class, pray for entry of judgment jointly and severally against Wells Fargo Defendants, and awarding Plaintiffs and the Class compensatory damages, statutory damages, treble damages, punitive damages, and reasonable attorney's fees and costs; and such other and further relief as this Court deems just and proper.

FIFTH CLAIM FOR RELIEF

107. Plaintiffs incorporate by reference paragraphs 1-106, as if set forth in full particularity herein.

108. Plaintiffs and the Class members delivered and entrusted their Private information to Defendants for the sole purpose of receiving services from Defendants, including, but not limited to, financial advisors, checking accounts, savings accounts, general banking services, including brokerage services all with having the ability to engage in financial transactions in safety.

109. Plaintiffs allege that Wells Fargo made representations and entered into contractual and

implied contractual relations regarding Wells Fargo's duty to safeguard Plaintiffs private information, including, but not limited to Wells Fargo's representations as set forth by Wells Fargo. (Exhibit A)

110. Plaintiffs contend that nowhere in the Wells Fargo Privacy Policy, does it allow Defendants to access Plaintiffs personal information for Wells Fargo to open accounts in Plaintiffs names without notifying customers, nor obtain emails, using customers names, or fraudulently conduct financial transactions without every notifying Plaintiffs.

111. Plaintiffs and Class Members allege that they entered into valid and enforceable agreements with Defendants whereby Defendants promised to provide goods or services to Plaintiffs and Class Members, and Plaintiffs and Class Members agreed to pay for those goods or services, including payment made with debit or credit cards.

112. Plaintiffs contend that they were never notified that Wells Fargo and its employees received incentives for "**gr-eight**" participation, or using Class Members private information to exploit Class Members for the monetary advantage of Wells Fargo or their employees, which private information included, inter alia, social security numbers which Wells Fargo classifies as "confidential" information. (<https://www.wellsfargo.com/privacy-security/privacy/social-security-number>. Last accessed on September 15, 2016)²

113. Plaintiffs allege that a material part of Wells Fargo's promise to provide services to Plaintiffs and Class Members was to adequately protect their personal and confidential information, and that Defendants intentionally, maliciously, and with intent to defraud, used Plaintiffs and Class Members social security numbers to open factious accounts, bundle products, sandbag, PIN, or in Gaming operations engaged in by Defendants, including executive's who may have included Carrie Tolstedt, who aided and abetted Defendants in hiding from regulators the fraudulent activity engaged in by Defendants.

114. Plaintiffs contend that Wells Fargo operated in a fiduciary position of trust, which position held them to a higher standard of performance than other corporations.

² Social Security numbers are classified as "Confidential" information under the Wells Fargo Information Security Policy. As such, Social Security numbers may only be accessed by and disclosed to Wells Fargo team members and others with a legitimate business "need to know" in accordance with applicable laws and regulations. Social Security numbers, whether in paper or electronic form, are subject to physical, electronic, and procedural safeguards, and must be stored, transmitted, and disposed of in accordance with the provisions of the Information Security Policy applicable to Confidential information. These restrictions apply to all Social Security numbers collected or retained by Wells Fargo in connection with customer, employee, or other relationships.

115. Plaintiffs assert that in its privacy policy, Wells Fargo expressly promised Plaintiffs and Class Members that it would protect Plaintiffs' and Class Members' personal and confidential information.

116. Plaintiffs contend that the contracts required Wells Fargo to safeguard Plaintiffs' and Class Members' private and confidential information to prevent its disclosure and/or unauthorized access.

117. Plaintiffs allege that a meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide their private and confidential information to Wells Fargo, in exchange for Wells Fargo's agreement to, among other things, protect their private and confidential information.

118. Plaintiffs assert that Wells Fargo failed to protect and safeguard Plaintiffs' and the Class Members' private and confidential information, as agreed to between the parties, and that this failure to protect the confidential and private information of Plaintiffs and Class Members was known to the highest ranking executive members of Wells Fargo, which may have included Carrie Tolstedt.

119. Plaintiffs allege that Wells Fargo's failure to meet these promises and obligations constitutes an express breach of contract.

120. Plaintiffs allege that Wells Fargo breached the contracts by failing to implement sufficient security measures to protect Plaintiffs' and the Class Members' private and confidential information, as described herein, as well as actively "mining" customers private information to use as Wells Fargo saw fit in order to maximize its own profit.

121. Wells Fargo's breach of its fiduciary duty to safeguard the confidential and private information of Plaintiffs and Class Members, and allowing access to its data security by Wells Fargo employees, constituted a breach of contract and Defendant's promise to supply adequate security and maintain customers' privacy, when in fact Wells Fargo neither supplied adequate security nor instituted adequate procedures to maintain customers' privacy.

122. Plaintiffs further allege that as a direct and proximate result of Wells Fargo's breach, Plaintiffs and Class Members suffered actual identity theft, as well as damages in the form of (i) improper disclosure of their private and confidential information; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them

by the data breach; (iii) the value of their time spent mitigating identity theft and/or identity fraud, and/or the increased risk of identity theft and/or identity fraud; (iv) and deprivation of the value of their private and confidential information, for which there is a well-established national and international market. These damages were within the contemplation of Wells Fargo and the Plaintiffs at the time that they contracted.

123. Plaintiffs contend that Wells Fargo breached its duty to safeguard their customers' privacy, and thereafter intentionally failed to inform Plaintiffs and Class members of the data breach/intentional theft and use of confidential information by Defendants.

124. The Utah Supreme Court has held that breach of contract, standing alone, does not call for punitive damages even if intentional and unjustified, but such damages are allowable if there is some independent tort indicating malice, fraud or wanton disregard for the rights of others. Hal Taylor Assocs v. Unionamerica, Inc., 657 P.2d 743, 750 (Utah 1982); See also Dold v. Outrigger Hotel, 54 Hawaii 18, 501 P.2d 368 (1972); Temmen v. Kent-Brown Chevrolet Co., 227 Kan. 45, 605 P.2d 95 (1980); Jackson v. Glasgow, Okla. Ct. App., 622 P.2d 1088 (1980). Plaintiffs contend, upon information and belief, that Wells Fargo management encouraged the theft by outrageous demands on employees, and executive officers being fully aware of the fraudulent activity transpiring under various programs to boost profits such as the “**gr-eight**” programs, calls for punitive damages. Plaintiffs contend that likewise Wells Fargo's failure to implement tighter security and oversight of corporate activities, coupled with its activation of programs which not only encouraged the illegal activity, but also rewarded the activity, call for punitive damages.

125. Plaintiffs contend that the wanton refusal to notify customers of the illegal, unethical activity of Wells Fargo for over a year since Wells Fargo was sued by Los Angeles, warrants the imposition of punitive damages against Defendants pursuant to the independent intentional torts committed by the Defendants.

126. Plaintiffs additionally contend that during the time of bailment, Defendants owed Plaintiffs and the Class members a duty to safeguard their information properly and maintain reasonable security procedures and practices to protect such information (as set forth in Wells Fargo's privacy policies).

127. Plaintiffs allege Defendant Wells Fargo intentionally breached this duty by allowing

access to the confidential information and allowing its own employees to fraudulently use customers' private and confidential information.

128. Plaintiffs assert that as a result of these breaches of duty, breach of contract, and breach of bailment, Plaintiffs and the Class members have suffered harm and damage in an amount to be proven at the time of trial.

WHEREFORE, Plaintiffs, on their own behalf and on behalf of the Class, pray for entry of judgment against Defendants Wells Fargo and Does 1-5,300, and awarding Plaintiffs and the Class compensatory damages, statutory damages, treble damages, punitive damages, and reasonable attorney's fees and costs; and such other and further relief as this Court deems just and proper.

SIXTH CLAIM FOR RELIEF

129. Plaintiffs incorporate by reference paragraphs 1-128 as if set forth with full particularity herein.

130. Plaintiffs allege that in order to benefit from Wells Fargo's services, Plaintiffs and Class Members were required to disclose their private and confidential information to Wells Fargo.

131. Plaintiffs allege that by providing Wells Fargo their private and confidential information, and upon Wells Fargo's acceptance of such information, Plaintiffs and Class Members entered into implied contracts with Wells Fargo whereby Wells Fargo was obligated to take reasonable steps to secure and safeguard that information, including compliance with federal banking and security laws.

132. Plaintiffs assert that a portion of the services purchased from Wells Fargo by Plaintiffs and Class Members necessarily included compliance with industry-standard measures with respect to the collection and safeguarding of Plaintiffs private and confidential information. Because Plaintiffs and Class Members were denied privacy protections that they paid for and were entitled to receive, Plaintiffs and Class Members incurred actual monetary damages in that they overpaid for the services purchased from Wells Fargo, including the overcharges on accounts, manipulation of accounting to obtain income for Wells Fargo.

133. Plaintiffs and Class Members have suffered additional injury in fact and actual damages, including monetary losses, arising from unauthorized bank account withdrawals and/or related bank fees charged to their accounts.

134. Plaintiffs and Class Members suffered additional damages arising from the costs associated with identity theft and the increased risk of identity theft caused by Wells Fargo's wrongful conduct, particularly given the incidents of actual misappropriation from Class Members' financial accounts, as detailed above.

135. A meeting of the minds occurred, as Plaintiffs and Class Members agreed to provide their private and confidential information and to pay Wells Fargo in exchange for Wells Fargo's agreement to, *inter alia*, provide services and otherwise take reasonable steps to protect Plaintiffs' and Class Members' private and confidential information.

136. Without such implied contracts, Plaintiffs and Class Members would not have provided their private and confidential information to Wells Fargo.

137. Plaintiffs allege that Wells Fargo failed to take reasonable steps to safeguard Plaintiffs' and Class Members' private and confidential information, and that as a result thereof, Wells Fargo allowed authorized and potentially unauthorized access to Plaintiffs' and Class Members' private and confidential information, and failed to take reasonable steps to safeguard that information, Wells Fargo breached its implied contracts with Plaintiffs and Class Members.

138. Plaintiffs assert that as a result of Wells Fargo's breach, Plaintiffs and Class Members suffered damages in the amount of the difference between the price they paid for Wells Fargo's services as promised and the actual diminished value of its services.

139. Additionally, as a result of Wells Fargo's breach, Plaintiffs and Class Members suffered actual identity theft, as well as damages in the form of (i) improper disclosure of their private and confidential information; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the data breach; (iii) the value of their time spent mitigating identity theft and/or identity fraud, and/or the increased risk of identity theft and/or identity fraud; (iv) and deprivation of the value of their private and confidential information, for which there is a well-established national and international market. These damages were within the contemplation of Wells Fargo and the Plaintiffs at the time that they contracted.

140. Plaintiffs and Class members were the owners and possessors of their private information. As the result of Defendants' wrongful conduct, Defendants have interfered with the Plaintiffs and Class members' rights to possess and control such property, to which they had a

superior right of possession and control at the time of conversion.

141. As a direct and proximate result of Defendants' conduct, Plaintiffs and the Class members suffered injury, damage, loss or harm and therefore seek compensatory damages.

142. Plaintiffs allege that in converting Plaintiffs and Class Members private information, Defendants have acted with malice, oppression and in conscious disregard of the Plaintiffs and Class members' rights. Plaintiffs, accordingly, seek an award of punitive damages on behalf of the Class.

143. Plaintiffs allege Defendants owed Plaintiffs a fiduciary duty and by allowing employees to steal their information, Defendants breached this fiduciary duty, as evidenced by numerous federal fines for improper banking activities. (Exhibit B)

144. Plaintiffs and Class members have suffered injury in fact and actual damages including lost money and property as a result of Wells Fargo's violations of the consumer fraud statutes.

145. Plaintiffs and the other Class members' injuries were proximately caused by Wells Fargo's fraudulent and deceptive behavior, which was conducted with reckless indifference toward the rights of others, such that an award of punitive damages is appropriate.

146. By this conduct, Wells Fargo violated the substantive consumer protection and unfair deceptive trade practices acts or statutes of the several States and the District of Columbia, as set forth above, whose laws do not materially differ from that of Utah, and do not conflict with each other for purposes of this action.

147. Additionally, despite the disclosure and dissemination of Plaintiffs and the Class members' private and confidential information occurring on a regular basis for over five (5) years, Wells Fargo, in violation of Utah's laws, failed to expeditiously and without unreasonable delay, notify Plaintiffs and the Class Members of the unlawful and unauthorized disclosure and dissemination of their private, personal and confidential information.

WHEREFORE, Plaintiffs, on their own behalf and on behalf of the Class, pray for entry of judgment jointly and severally against Defendants, and awarding Plaintiffs and the Class compensatory damages, statutory damages, treble damages, punitive damages, and reasonable attorney's fees and costs; and such other and further relief as this Court deems just and proper.

SEVENTH CLAIM FOR RELIEF

148. Plaintiffs incorporate the allegations in paragraphs 1-147, as if fully set forth herein.

149. Plaintiff's contend that The Fair Credit Reporting Act ("FCRA") requires consumer reporting agencies to adopt and maintain procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner fair and equitable to consumers while maintaining the confidentiality, accuracy, relevancy and proper utilization of such information. 15 U.S.C. § 1681(b).

150. The FCRA allows for a private right of action against any reporting agency for the negligent or willful violation of any duty imposed under the statute.

151. The FCRA defines a "consumer reporting agency" as:

Any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.

15 U.S.C. § 1681a(f).

152. FCRA defines a "consumer report" as:

[A]ny written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of establishing the consumer's eligibility for credit or insurance to be used primarily for personal, family, or household purposes; employment purposes, or any other purpose authorized under [15 U.S.C. §] 1681(b).

15 U.S.C § 1681a(d).

153. Wells Fargo is a consumer reporting agency as defined under the FCRA because Wells Fargo through third parties, for monetary fees, regularly engages, in part, in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties and/or uses interstate commerce for the purpose of preparing and/or furnishing consumer reports.

154. As a consumer reporting agency, Wells Fargo was (and continues to be) required to adopt and maintain procedures designed to protect and limit the dissemination of consumer credit, personnel, insurance and other information (such as Plaintiffs' and other Class Members' private and confidential information) in a manner fair and equitable to consumers, while

maintaining the confidentiality, accuracy, relevancy, and proper utilization of such information. Defendants, violated FCRA by failing to adopt and maintain such protective procedures which, in turn, directly and/or proximately resulted in the theft of Plaintiffs' and Class Members' private and confidential information and its wrongful dissemination.

155. On information and belief, Wells Fargo knowingly failed to adequately implement these proactive actions to secure and protect Plaintiffs' and Class Members' private and confidential information, and/or put itself in a position to immediately notify Plaintiffs and Class Members about the data breach.

156. As a direct and/or proximate result of Wells Fargo's willful and/or reckless violations of the FCRA as described above, Plaintiffs' and Class Members' private and confidential information was stolen and made accessible to unauthorized third parties.

157. As a direct and/or proximate result of Wells Fargo's willful and/or reckless violations of the FCRA, as described above, Plaintiffs and Class Members were (and continue to be) damaged in the form of, without limitation, expenses for credit monitoring and identity theft insurance, out-of-pocket expenses, anxiety, emotional distress, loss of privacy and other economic and non-economic harm.

158. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages including, (i) actual damages resulting from the identity theft; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the data breach; (iii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iv) deprivation of the value of their private and confidential information, for which there is a well-established national and international market; (v) anxiety and emotional distress; and (vi) statutory damages of not less than \$100, and not more than \$1,000, each, as well as attorneys' fees, litigation expenses and costs, pursuant to 15 U.S.C. §1681n(a).

WHEREFORE, Plaintiffs, on their own behalf and on behalf of the Class, pray for entry of judgment jointly and severally against Defendants, and awarding Plaintiffs and the Class compensatory damages, statutory damages, treble damages, punitive damages, and reasonable attorney's fees and costs; and such other and further relief as this Court deems just and proper.

EIGHTH CLAIM FOR RELIEF

159. Plaintiffs incorporate the allegations in paragraphs 1-158, as if fully set forth herein.

160. In the alternative to Count Seventh, above, Wells Fargo negligently violated the FCRA by failing to adopt and maintain procedures designed to protect and limit the dissemination of Plaintiffs' and Class Members' private and confidential information for the permissible purposes outlined by the FCRA which, in turn, directly and/or proximately resulted in the wrongful dissemination of Plaintiffs' and Class Members' private and confidential information.

161. Wells Fargo's action, by its pressure on employees, and refusing to enforce fiduciary duties because a fine is cheaper to pay than the profits they obtained, was reasonably foreseeable that Wells Fargo's failure to implement and maintain procedures to protect and secure Plaintiffs' and Class Members' private and confidential information would result in the unauthorized use by Wells Fargo of its customers' private and confidential information for no permissible purpose under the FCRA.

162. As a direct and/or proximate result of Wells Fargo's negligent violations of the FCRA, as described above, Plaintiffs' and Class Members' private and confidential information was essentially stolen and made accessible for unauthorized purposes by Wells Fargo executives and employees.

163. As a direct and/or proximate result of Wells Fargo's negligent violations of the FCRA, as described above, Plaintiffs and Class Members were (and continue to be) damaged in the form of, without limitation, actual identity theft, expenses for credit monitoring and identity theft insurance, anxiety, emotional distress, loss of privacy, and other economic and noneconomic harm.

164. Plaintiffs and Class Members, therefore, are entitled to compensation for their actual damages, including, (i) actual damages resulting from the identity theft; (ii) out-of-pocket expenses incurred to mitigate the increased risk of identity theft and/or identity fraud pressed upon them by the data breach; (iii) the value of their time spent mitigating identity theft and/or identity fraud and/or the increased risk of identity theft and/or identity fraud; (iv) deprivation of the value of their private and confidential information, for which there is a well-established national and international market; (v) anxiety and emotional distress; and (viii) attorneys' fees,

litigation expenses and costs, pursuant to 15 U.S.C. § 1681o(a).

WHEREFORE, Plaintiffs, on their own behalf and on behalf of the Class, pray for entry of judgment jointly and severally against Defendant Wells Fargo, and awarding Plaintiffs and the Class compensatory damages, statutory damages, treble damages, punitive damages, and reasonable attorney's fees and costs; and such other and further relief as this Court deems just and proper.

NINTH CLAIM FOR RELEIF COUNT

165. Plaintiffs incorporate the allegations in paragraphs 1-164 as if fully set forth herein.

166. The Declaratory Judgment Act ("DJA") states:

"In a case of actual controversy within its jurisdiction ... any court of the United States, upon the filing of an appropriate pleading, may declare the rights and other legal relations of any interested party seeking such declaration, whether or not further relief is or could be sought. Any such declaration shall have the force and effect of a final judgment or decree and shall be reviewable as such."

28 U.S.C. § 2201(a).

167. In the case at hand, there is an actual controversy between the parties of sufficient immediacy and reality to warrant the issuance of a declaratory judgment, due to the imminence of harm facing Plaintiffs and Class Members. As set forth above, Class Members have already suffered identity theft and damages as a result of the data breach, and the perpetrators are still at large with Class Members' private and confidential information.

168. Plaintiffs seek a declaration that Wells Fargo has breached a contract between those entities and Plaintiffs and Class Members by allowing unauthorized individuals were allowed access to personal financial data, an/or authorized parties engaged in fraudulent activities in accessing and misusing fiduciary, confidential information.

169. Plaintiffs further seek a declaration that due to the imminence and likelihood of harm to Plaintiffs and Class Members, Wells Fargo be ordered to pay for mitigation in the form of legitimate and adequate credit monitoring, identity theft protection, and identity theft

insurance, and also be ordered to indemnify Plaintiffs and Class Members for future harm.

TENTH CLAIM FOR RELIEF

170. Plaintiffs incorporate by reference all allegations of the preceding paragraphs as though fully set forth herein.

171. Plaintiffs and members of the Class paid Wells Fargo excessive fees, fines, collection costs, had their personal information misused by Wells Fargo for the benefit of Wells Fargo and its employees.

172. Upon information and belief, executives and employees of Wells Fargo received bonuses in the millions of dollars, including severance fees of over one hundred million dollars, for their participation in the “gr-eight” program where Plaintiffs were the victims of fraudulent activities.

173. Defendant and its employees have been unjustly enriched at the expense of Plaintiffs and the Class and its retention of this benefit under the circumstances would be inequitable.

174. Plaintiffs seek an order requiring Defendant to make restitution to them and the other members of the Class, including a clawback provision for those who profited personally from the illegal behavior.

WHEREFORE, Plaintiffs, on their own behalf and on behalf of the Class, pray for an

Order against Defendants jointly and severally as follows:

A. Finding that this action satisfies the prerequisites for maintenance as a class action set forth in Fed.R.Civ.P. 23, and certifying the Class defined herein;

B. Designating Plaintiffs as the representatives of the Class and their undersigned counsel as Class Counsel;

C. Entering judgment jointly and severally in favor of Plaintiffs and the Class and against Wells Fargo Defendants;

D. Entering a declaration that Defendants have breached a contract between it and Plaintiffs and Class Members by allowing unauthorized third-parties to access personal financial data, and/or allowed authorized personnel to knowingly misuse, misappropriate, and engage in fraudulent activity with respect to Plaintiffs and Class Members confidential information, and that Defendants be ordered to pay for mitigation in the form of clawbacks from employees who profited from the illegal activity, along with adequate credit monitoring, identity theft protection, and identity theft insurance, and also be ordered to indemnify Plaintiffs and Class Members for future harm; and

E. Granting all such further and other relief as the Court deems just and appropriate.

PRAYER FOR RELIEF WHEREFORE Plaintiffs pray for judgment as follows:

- A. For an Order certifying this action as a class action and appointing Plaintiffs and their Counsel to represent the Class;
- B. For equitable relief enjoining Defendants, jointly and severally, from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs and Class members' private information, and from refusing to issue prompt, complete and accurate disclosures to the Plaintiffs and Class members;
- C. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of Defendants' wrongful conduct, including clawback provisions;
- D. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined for Defendants knowing theft, engagement in a continuous pattern of fraud, conspiracy to commit fraud, cleaning up each customers' account from inaccurate reporting to credit agencies ;
- E. For an award of punitive damages;
- F. For an award of costs of suit and attorneys' fees, as allowable by law; and
- G. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial of their claims to the extent authorized by law.

Dated: September 15, 2016

Christensen Young & Associates, PLLC
/s/ Steven A. Christensen

Steven A. Christensen

Zane L. Christensen

Christensen Young & Associates, PLLC

9980 So. 300 West, #200

Sandy, Utah, 84070

(801) 676-6447

schristensen@christensenyoung.com

zane@christensenyounglaw.com

EXHIBIT A

Wells Fargo U.S. Consumer Privacy Notice

This notice is effective as of November 1, 2013.

FACTS	WHAT DOES WELLS FARGO DO WITH YOUR PERSONAL INFORMATION?		
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.		
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: Social Security number and employment information Account balances and transaction history Credit history and investment experience		
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Wells Fargo chooses to share; and whether you can limit this sharing.		
Reasons we can share your personal information		Does Wells Fargo share?	Can you limit this sharing?
For our everyday business purposes — such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus		Yes	No
For our marketing purposes — with service providers we use to offer our products and services to you (please see below to limit the ways in which we contact you)		Yes	No

Reasons we can share your personal information	Does Wells Fargo share?	Can you limit this sharing?
For joint marketing with other financial companies	No	We don't share
For our affiliates' everyday business purposes — information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes — information about your creditworthiness	Yes	Yes
For our affiliates to market to you	Yes	Yes
For nonaffiliates to market to you	No	We don't share
To limit our sharing	<p>Call 1-888-528-8460 — our menu will prompt you through your choices.</p> <p>Online banking customers — log on to a secure session at wells Fargo.com, and choose Change Privacy Preferences under the Account Services tab.</p> <p>Please note:</p> <p>If you are a new customer, we can begin sharing your information 30 days from the date we sent this notice. When you are no longer our customer, we can continue to share your information as described in this notice. However, you can contact us at any time to limit our sharing.</p>	
To limit direct marketing	<p>To limit our direct marketing to you by mail or telephone, call 1-888-528-8460 — our menu will guide you through your choices.</p> <p>Online banking customers — log on to a secure session at wells Fargo.com, and choose Change Privacy Preferences under the Account Services tab.</p> <p>Please note:</p> <p>A Do Not Call election is effective for five years, or while you are an active consumer customer, if longer than five years. The Do Not Mail election is effective for three years. You may continue to receive marketing information in regular account mailings and statements</p>	

	when you visit us online or at an ATM. You may also be contacted to service your account or participate in surveys. If you have an assigned client manager or team, they may continue to contact you to assist you in managing your portfolio or account relationship.
Questions?	Call 1-800-TO-WELLS (1-800-869-3557) or go to wellsfargo.com/privacy-security
Who we are	
Who is providing this notice?	Wells Fargo U.S. companies that use Wells Fargo in their names and other companies listed in the Wells Fargo U.S. legal entities section below.
What we do	
How does Wells Fargo protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. For more information, visit wellsfargo.com/privacy-security
How does Wells Fargo collect my personal information?	<p>We collect your personal information, for example, when you:</p> <ul style="list-style-type: none"> Open an account or make deposits or withdrawals from your accounts Apply for a loan or use your credit or debit card Seek advice about your investment <p>We also collect your personal information from others, such as credit bureaus, affiliates, or other companies.</p>
Why can't I limit all sharing?	<p>Federal law gives you the right to limit only:</p> <ul style="list-style-type: none"> Sharing for affiliates' everyday business purposes — information about your creditworthiness

Who we are	
	<p>Affiliates from using your information to market to you</p> <p>Sharing for nonaffiliates to market to you</p> <p>State laws and individual companies may give you additional rights to limit sharing. See below for more on your rights under state law.</p>
What happens when I limit sharing for an account I hold jointly with someone else?	<p>Your choices will apply individually unless you tell us otherwise. Any account holder may express a privacy preference on behalf of the other joint account holders.</p>
Definitions	
Affiliates	<p>Companies related by common ownership or control. They can be financial and non-financial companies.</p> <p>Our affiliates include financial companies with Wells Fargo in their name such as Wells Fargo Bank, N.A., Wells Fargo Insurance, Inc., and Wells Fargo Advisors, LLC.</p>
Nonaffiliates	<p>Companies not related by common ownership or control. They can be financial and non-financial companies.</p> <p>Wells Fargo does not share with nonaffiliates so they can market to you.</p>
Joint marketing	<p>A formal agreement between nonaffiliated financial companies that together market financial products or services to you.</p> <p>Wells Fargo does not jointly market.</p>
Other important information	

Other important information

Important notice about credit reporting: We may report information about your account(s) to credit bureaus and/or consumer reporting agencies. Late payments, missed payments, or other defaults on your account(s) may be reflected in your credit report and/or consumer report.

Do Not Call Policy: This Privacy Policy constitutes Wells Fargo's Do Not Call Policy under the Telephone Consumer Protection Act for all consumers. Wells Fargo maintains an internal Do Not Call preference list. Do Not Call requests will be honored within 30 days and will be effective for at least five years from the date of request. No telemarketing calls will be made to residential or cellular phone numbers that appear on the Wells Fargo Do Not Call list.

Nevada residents: We are providing you this notice pursuant to state law. You may be placed on our internal Do Not Call List by following the directions in the *To limit direct marketing* section. For more information, contact us at **1-800-869-3557**; nevadanoticeinfo@wellsfargo.com, or Wells Fargo, P.O. Box 5277, Sioux Falls, SD 57117-5277. Or, contact the Bureau of Consumer Protection, Office of the Nevada Attorney General, 555 E. Washington St., Suite 3900, Las Vegas, NV 89101; **702-486-3132**; BCPINFO@ag.state.nv.us.

Vermont: We automatically treat customers with a Vermont mailing address as having limited sharing with our affiliates as provided on page one.

Trust or fiduciary accounts: Trust or fiduciary accounts for which Wells Fargo is the trustee or service provider, including employer-sponsored retirement accounts, are protected under special rules of confidentiality. Information on these accounts is not shared for marketing purposes without specific consent.

Wells Fargo Advisors financial advisors: If your financial advisor's affiliation with Wells Fargo Advisors ends and they join a non-affiliated securities broker-dealer, your financial advisor may be permitted to use limited information to contact you to join their new firm, as a usual means to continue to service and maintain your accounts. The information they may use is limited to your name, address, email address, phone number, and account title.

Wells Fargo U.S. legal entities and businesses covered by this notice

Wells Fargo U.S. banks and companies with “Wells Fargo” in their names, including Wells Fargo Advisors, LLC; Wells Fargo Bank, N.A. doing business as Flatiron Capital; as well as American Mortgage Network, LLC, doing business as Vertice; and Abbot Downing, a Wells Fargo Business.

This Privacy Notice also describes the privacy practices of First Clearing, LLC (“First Clearing”), which is an affiliated clearing firm of Wells Fargo Advisors, LLC. First Clearing does not market to holders of accounts carried by First Clearing or provide information regarding such accounts or regarding your creditworthiness to other Wells Fargo companies for their own marketing or everyday business purposes, and the choices in this notice do not apply to First Clearing.

The following legal entities and businesses are **not** covered by this notice and have separate privacy notices:

Wells Fargo Financial National Bank

Wells Fargo Funds

Wells Fargo Advisors Financial Network, LLC

Any insurance company, insurance agency, or insurance brokerage or other company, which has its own privacy notices

Businesses which have provided a separate privacy notice governing specified accounts or relationships

Wells Fargo Asset Management is a trade name used by the asset management businesses of Wells Fargo & Company. Wells Fargo Funds Management, LLC, a wholly owned subsidiary of Wells Fargo & Company, provides investment advisory and administrative services for Wells Fargo Funds. Other affiliates of Wells Fargo & Company provide subadvisory and other services for the funds. The funds are distributed by **Wells Fargo Funds Distributor, LLC**, Member [FINRA](#), an affiliate of Wells Fargo & Company. 242059 04-16

EXHIBIT B

**UNITED STATES OF AMERICA
CONSUMER FINANCIAL PROTECTION BUREAU**

ADMINISTRATIVE PROCEEDING

2016-CFPB-0015

In the Matter of:

WELLS FARGO BANK, N.A.

CONSENT ORDER

The Consumer Financial Protection Bureau (Bureau) has reviewed the sales practices of Wells Fargo Bank, N.A. (Respondent, as defined below) and determined that it has engaged in the following acts and practices: (1) opened unauthorized deposit accounts for existing customers and transferred funds to those accounts from their owners' other accounts, all without their customers' knowledge or consent; (2) submitted applications for credit cards in consumers' names using consumers' information without their knowledge or consent; (3) enrolled consumers in online-banking services that they did not request; and (4) ordered and activated debit cards using consumers' information without their knowledge or consent. The Bureau has concluded that such acts violate §§ 1031 and 1036(a)(1)(B) of the Consumer Financial Protection Act of 2010 (CFPA), 12 U.S.C. §§ 5531 and 5536(a)(1)(B). Under §§ 1053 and 1055 of 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, 5565.

II Stipulation

2. Respondent has executed a “Stipulation and Consent to the Issuance of a Consent Order” (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 the findings of facts and 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. **“Affected Consumers”** means any consumer subjected to any of the Improper Sales Practices.
 - b. **“Board”** means Respondent’s duly-elected and acting Board of Directors.
 - c. **“California Enforcement Action”** means the lawsuit styled *People v. Wells Fargo & Co., et al.*, Los Angeles Superior Court, Case No. BC580778, filed by the Office of the Los Angeles City Attorney.
 - d. **“Community Bank Regional Bank Branch Network”** means the Respondent’s retail-branch operations within Respondent’s Regional Bank group.

e. **“Effective Date”** means the date on which this Order is issued.

f. **“Improper Sales Practices”** means any of the following in the Community Bank Regional Bank Branch Network:

- (1) opening any account without the consumer’s consent;
- (2) transferring funds between a consumer’s accounts without the consumer’s consent;
- (3) applying for any credit card without the consumer’s consent;
- (4) issuing any debit card without the consumer’s consent; and
- (5) enrolling any consumer in online-banking services without the consumer’s consent.

g. **“Los Angeles City Attorney”** means the Office of the Los Angeles City Attorney.

h. **“Regional Director”** means the Regional Director for the West Region for the Office of Supervision for the Consumer Financial Protection Bureau, or his/her delegate.

i. **“Related Consumer Action”** means a private action by or on behalf of one or more consumers or an enforcement action by a governmental agency other than the California Enforcement Action, brought against Respondent based on substantially the same facts as described in Section IV of this Consent Order.

j. **“Relevant Period”** includes the period from January 1, 2011, to the Effective Date.

k. **“Respondent”** means Wells Fargo Bank, N.A. and its successors and assigns.

IV Bureau Findings and Conclusions

The Bureau finds the following:

4. Respondent is a national bank headquartered in Sioux Falls, South Dakota. Respondent is an insured depository institution with assets greater than \$10 billion within the meaning of 12 U.S.C. § 5515(a).
5. Respondent is a “covered person” under 12 U.S.C. § 5481(6).
6. During the Relevant Period, Respondent offered a broad array of consumer financial products and services, including mortgages, savings and checking accounts, credit cards, debit and ATM cards, and online-banking services.
7. Respondent sought to distinguish itself in the marketplace as a leader in “cross-selling” banking products and services to its existing customers.
8. Respondent set sales goals and implemented sales incentives, including an incentive-compensation program, in part to increase the number of banking products and services that its employees sold to its customers.
9. Thousands of Respondent’s employees engaged in Improper Sales Practices to satisfy sales goals and earn financial rewards under Respondent’s incentive-compensation program. During the Relevant Period, Respondent terminated roughly 5,300 employees for engaging in Improper Sales Practices.
10. Respondent’s employees engaged in “simulated funding.” To qualify for incentives that rewarded bankers for opening new accounts that were funded shortly after opening, Respondent’s employees opened deposit accounts without consumers’ knowledge or consent and then transferred funds from consumers’ authorized accounts

to temporarily fund the unauthorized accounts in a manner sufficient for the employee to obtain credit under the incentive-compensation program.

11. Respondent's employees submitted applications for and obtained credit cards for consumers without the consumers' knowledge or consent.

12. Respondent's employees used email addresses not belonging to consumers to enroll consumers in online-banking services without their knowledge or consent.

13. Respondent's employees requested debit cards and created personal identification numbers (PINs) to activate them without the consumer's knowledge or consent.

14. During the Relevant Period, Respondent's employees opened hundreds of thousands of unauthorized deposit accounts and applied for tens of thousands of credit cards for consumers without consumers' knowledge or consent.

15. Respondent has performed an analysis to assess the scope of Improper Sales Practices that occurred between May 2011 and July 2015, including the number of potential instances of such practices.

Findings and Conclusions as to Unauthorized Deposit Accounts & Simulated Funding

16. Respondent's analysis concluded that its employees opened 1,534,280 deposit accounts that may not have been authorized and that may have been funded through simulated funding, or transferring funds from consumers' existing accounts without their knowledge or consent. That analysis determined that roughly 85,000 of those accounts incurred about \$2 million in fees, which Respondent is in the process of refunding. The fees included overdraft fees on linked accounts the consumers already

had, monthly service fees imposed for failure to keep a minimum balance in the unauthorized account, and other fees.

17. Section 1036(a)(1)(B) of the CFPA prohibits “unfair” acts or practices. 12 U.S.C. § 5536(a)(1)(B). An act or practice is unfair if it causes or is likely to cause consumers substantial injury that is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or to competition. 12 U.S.C. § 5531(c)(1).

18. By opening unauthorized deposit accounts and engaging in acts of simulated funding, Respondent caused and was likely to cause substantial injury to consumers that was not reasonably avoidable, because it occurred without consumers’ knowledge, and was not outweighed by countervailing benefits to consumers or to competition.

19. Section 1036(a)(1)(B) of the CFPA prohibits “abusive” acts or practices. 12 U.S.C. § 5536(a)(1)(B). An act or practice is abusive if it materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service. 12 U.S.C. § 5531(d)(1). Additionally, an act or practice is abusive if it takes unreasonable advantage of the inability of the consumer to protect his or her interests in selecting or using a consumer financial product or service. 12 U.S.C. § 5531(d)(2)(B).

20. Respondent’s acts of opening unauthorized deposit accounts and engaging in simulated funding materially interfered with the ability of consumers to understand a term or condition of a consumer financial product or service, as they had no or limited knowledge of those terms and conditions, including associated fees.

21. Additionally, Respondent’s acts of opening unauthorized deposit accounts and engaging in simulated funding took unreasonable advantage of consumers’ inability

to protect their interests in selecting or using consumer financial products or services, including interests in having an account opened only after affirmative agreement, protecting themselves from security and other risks, and avoiding associated fees.

22. Therefore, Respondent engaged in “unfair” and “abusive” acts or practices that violate §§ 1031(c)(1), (d)(1), (d)(2)(B), and 1036(a)(1)(B) of the CFPA. 12 U.S.C. §§ 5531(c)(1), (d)(1), (d)(2)(B), 5536(a)(1)(B).

Findings and Conclusions as to Unauthorized Credit Cards

23. Respondent’s analysis concluded that its employees submitted applications for 565,443 credit-card accounts that may not have been authorized by using consumers’ information without their knowledge or consent. That analysis determined that roughly 14,000 of those accounts incurred \$403,145 in fees, which Respondent is in the process of refunding. Fees incurred by consumers on such accounts included annual fees and overdraft-protection fees, as well as associated finance or interest charges and other late fees.

24. Section 1036(a)(1)(B) of the CFPA prohibits “unfair” acts or practices. 12 U.S.C. § 5536(a)(1)(B). An act or practice is unfair if it causes or is likely to cause consumers substantial injury that is not reasonably avoidable and is not outweighed by countervailing benefits to consumers or to competition. 12 U.S.C. § 5531(c)(1).

25. By applying for and opening credit-card accounts using consumers’ information without their knowledge or consent, Respondent caused and was likely to cause substantial injury that was not reasonably avoidable, because it occurred without consumers’ knowledge, and was not outweighed by countervailing benefits to consumers or competition.

26. Section 1036(a)(1)(B) of the CFPA prohibits “abusive” acts or practices. 12 U.S.C. § 5536(a)(1)(B). An act or practice is abusive if it materially interferes with the ability of a consumer to understand a term or condition of a consumer financial product or service. 12 U.S.C. § 5531(d)(1). Additionally, an act or practice is abusive if it takes unreasonable advantage of the consumer’s inability to protect his or her interests in selecting or using a consumer financial product or service. 12 U.S.C. § 5531(d)(2)(B).

27. Respondent’s acts of opening credit-card accounts using consumers’ information without their knowledge or consent materially interfered with the ability of consumers to understand a term or condition of a consumer financial product or service, as they had no or limited knowledge of those terms and conditions, including associated fees.

28. Additionally, Respondent’s acts of opening credit-card accounts using consumers’ information without their knowledge or consent took unreasonable advantage of the consumers’ inability to protect their interests in selecting or using a consumer financial product or service.

29. Therefore, Respondent engaged in “unfair” and “abusive” acts or practices that violate §§ 1031(c)(1), (d)(1), (d)(2)(B), and 1036(a)(1)(B) of the CFPA. 12 U.S.C. §§ 5531(c)(1), (d)(1), (d)(2)(B), 5536(a)(1)(B).

Findings and Conclusions as to Unauthorized Enrollment into Online-Banking Services

30. During the Relevant Period, Respondent’s employees used email addresses not belonging to consumers to enroll consumers in online-banking services without their knowledge or consent.

31. Section 1036(a)(1)(B) of the CFPA prohibits “abusive” acts or practices. 12 U.S.C. § 5536(a)(1)(B). An act or practice is abusive if it takes unreasonable advantage of the consumer’s inability to protect his or her interests in selecting or using a consumer financial product or service. 12 U.S.C. § 5531(d)(2)(B).

32. Respondent’s acts of enrolling consumers in online-banking services without their knowledge or consent took unreasonable advantage of consumers’ inability to protect their interests in selecting or using a consumer financial product or service, including interests in having these products or services activated only after affirmative agreement and protecting themselves from security and other risks.

33. Therefore, Respondent engaged in “abusive” acts or practices that violate §§ 1031(d)(2)(B) and 1036(a)(1)(B) of the CFPA. 12 U.S.C. §§ 5531(d)(2)(B), 5536(a)(1)(B).

Findings and Conclusions as to Unauthorized Debit Cards

34. During the relevant period, Respondent’s employees requested debit cards and created PINs to activate them without consumers’ knowledge or consent.

35. Section 1036(a)(1)(B) of the CFPA prohibits “abusive” acts or practices. 12 U.S.C. § 5536(a)(1)(B). An act or practice is abusive if it takes unreasonable advantage of the consumer’s inability to protect his or her interests in selecting or using a consumer financial product or service. 12 U.S.C. § 5531(d)(2)(B).

36. Respondent’s acts of issuing debit cards to consumers without their knowledge or consent took unreasonable advantage of consumers’ inability to protect their interests in selecting or using a consumer financial product or service. 12 U.S.C. § 5531(d)(2)(B).

37. Therefore, Respondent engaged in “abusive” acts that violate §§ 1031(d)(2)(B) and 1036(a)(1)(B) of the CFPA, 12 U.S.C. §§ 5531(d)(2)(B), 5536(a)(1)(B).

ORDER

V Conduct Provisions

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

38. Respondent and its officers, agents, servants, employees, and attorneys who have actual notice of this Consent Order, whether acting directly or indirectly, may not violate §§ 1031 and 1036 of the CFPA, 12 U.S.C. §§ 5531, 5536, by engaging in Improper Sales Practices.

VI Independent Consultant’s Report and Compliance Plan

IT IS FURTHER ORDERED that:

39. Within 45 days of the Effective Date, Respondent must select an independent consultant with specialized experience in consumer-finance-compliance issues to conduct an independent review of Respondent’s sales practices within the Community Bank Regional Bank Branch Network related to deposit accounts, credit-card accounts, unsecured lines of credit, and related products and services (Independent Consultant’s Review). Respondent must submit the name of the independent consultant to the Regional Director for non-objection. Upon receipt of non-objection from the Regional Director, the Bank must retain the independent consultant. The Independent Consultant’s Review must assess whether Respondent’s current policies and procedures are reasonably designed to ensure that Respondent’s sales practices comply with all applicable Federal consumer financial laws as defined in 12 U.S.C. § 5481(14), and that Respondent’s employees do not engage in Improper Sales Practices.

40. The Independent Consultant's Review must include but will not be limited to:

a. whether Respondent's employees are required to undergo training reasonably designed to prevent Improper Sales Practices and other sales-integrity violations; whether such training is adequate, complete, and timely updated, provided when employees join Respondent, and repeated at sufficient recurring intervals during their employment to reinforce such training; whether training records are complete, accurate and adequate; and whether employees are informed of an obligation to report all sales-integrity issues internally through an "ethics hotline" or similar mechanism;

b. whether Respondent's monitoring policies and procedures ensure that Respondent monitors employees' sales practices proactively, and that Respondent devotes sufficient personnel and resources to monitor those practices appropriately;

c. whether Respondent has adequate policies and procedures for (i) receiving, retaining, and addressing consumer inquiries or complaints; (ii) receiving, retaining, and addressing employee allegations of Improper Sales Practices or any other allegations of sales-integrity violations; (iii) tracking and addressing indicators of potential Improper Sales Practices or any other sales-integrity violations; and (iv) identifying and remediating consumers for Improper Sales Practices or other sales-integrity violations identified after the Effective Date, as well as for correcting any related systemic issues identified after the Effective Date;

d. whether Respondent's policies and procedures related to sales of deposit accounts, credit cards, unsecured lines of credit, and related products and services are reasonably designed to ensure consumer consent is obtained before any such product is sold or issued to a consumer. The Independent Consultant's Review

must include, but not be limited to, whether Respondent has adequate policies and procedures for capturing and retaining consumer signatures and other evidence of consent for such products and services, for providing a grace period before assessing fees on any deposit account, and for closing accounts in which there is no customer-initiated activity during the grace period without assessing fees; and

e. whether Respondent's performance-management and sales goals for its employees are consistent with the objective of preventing Improper Sales Practices and other sales-integrity violations.

41. Within 180 days of the retention of the independent consultant, the independent consultant must prepare a written report (Independent Consultant's Report) detailing the findings of the review and provide the Independent Consultant's Report to the Board or a committee thereof.

42. Within 90 days of receiving the Independent Consultant's Report, the Board or a committee thereof must:

a. In consultation with the independent consultant, 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 Independent Consultant's Report and the Compliance Plan to the Regional Director.

43. The Regional Director may, in his or her discretion, make a determination of non-objection to the Compliance Plan or direct Respondent to revise it. If the Regional Director directs Respondent to revise the Compliance Plan, the Board or a committee thereof must make the requested revisions to the Compliance Plan, have the

independent consultant review the revised Compliance Plan for adequacy, accuracy, effectiveness, and completeness, and resubmit the revised Compliance Plan and the independent consultant's review of the revised Compliance Plan to the Regional Director within 60 days of the date that the Regional Director directs the Company to revise the Compliance Plan. The Regional Director may, in his or her discretion, consult with the Los Angeles City Attorney in arriving at a determination of non-objection to the Compliance Plan or direction to Respondent to revise the Compliance Plan.

44. After receiving notification that the Regional 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 and have the independent consultant review and assess compliance with the Compliance Plan and validate that the Compliance Plan has been properly executed; the results of such review should be submitted to the Regional Director within 30 days after completion.

VII Role of the Board

IT IS FURTHER ORDERED that:

45. The Board or a committee thereof must review all submissions (including plans, reports, programs, policies, and procedures) required by this Consent Order before submission to the Bureau.

46. Although this Consent Order requires Respondent to submit certain documents for the review or non-objection by the Regional Director, the Board will have the ultimate responsibility for proper and sound management of Respondent and for

ensuring that Respondent complies with Federal consumer financial law and this Consent Order.

47. In each instance that this Consent Order requires the Board or a committee thereof to ensure adherence to, or perform certain obligations of Respondent, the Board or a committee thereof 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 or a committee thereof 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 directives from the Board or a committee thereof related to this Section.

VIII Order to Pay Redress

IT IS FURTHER ORDERED that:

48. Respondent has retained the services of an independent third-party consulting firm (which is not the independent consultant referred to in Section VI) to identify consumers who have incurred fees or other charges as a result of Improper Sales Practices.

49. Within 10 days of the Effective Date, Respondent must reserve or deposit into a segregated deposit account an amount not less than \$5 million, for the purpose of providing redress to Affected Consumers as required by this Section.

50. Within 90 days of the Effective Date, Respondent must submit to the Regional Director for review and non-objection the comprehensive written plan for

providing redress consistent with this Consent Order (Redress Plan). The Regional Director may, in his or her discretion, make a determination of non-objection to the Redress Plan or direct Respondent to revise it. If the Regional Director directs Respondent to revise the Redress Plan, Respondent must make the revisions and resubmit the Redress Plan to the Regional Director within 45 days. After receiving notification that the Regional Director has made a determination of non-objection to the Redress Plan, Respondent must implement and adhere to the steps, recommendations, deadlines, and timeframes outlined in the Redress Plan.

51. The Redress Plan must:

- a. identify all Affected Consumers, except insofar as it is impracticable to do so, as well as the types and amounts of any fees or charges incurred by Affected Consumers as a result of the Improper Sales Practices, and state the means by which Affected Consumers have been identified and by which the fees or charges they incurred have been calculated;
- b. describe procedures by which Respondent will notify Affected Consumers who were subject to any of the Improper Sales Practices described in paragraph 3.f of this Order, including the form of the notification such consumers will receive;
- c. describe the process for providing redress to Affected Consumers and identify the dollar amount of redress for each category of Affected Consumers;
- d. detail how Respondent will locate Affected Consumers for payment of redress, and the steps Respondent will take with respect to consumers whose redress payments are returned as undeliverable or not cashed within a prescribed time period;

e. state the manner in which redress will be provided to each such Affected Consumer, and the form of redress; and

f. provide the form of the letter or notice that will be sent to such Affected Consumers notifying them of the redress.

52. Within 120 days after completing the Redress Plan, Respondent's Internal Audit department must review and assess compliance with the terms of the Redress Plan (Redress Plan Review) and validate that the Redress Plan has been properly executed.

53. Within 30 days after completion of the Redress Plan Review, Respondent must prepare and submit to the Regional Director a report summarizing the results of the Redress Plan Review.

54. After completing the Redress Plan, if the amount of redress provided to Affected Consumers is less than \$5 million, Respondent may recoup any remaining funds up to the amount Respondent paid to Affected Consumers before the submission of the Redress Plan as redress for fees or charges those Affected Consumers incurred as a result of the Improper Sales Practices. Respondent must, within 30 days of the completion of the Redress Plan, pay to the Bureau, by wire transfer to the Bureau or to the Bureau's agent and according to the Bureau's wiring instructions, any remaining funds not recouped by Respondent under this paragraph.

55. The Bureau may use these remaining funds to pay additional redress to Affected Consumers. Upon receiving a written request from Respondent, the Bureau may provide Respondent with information concerning additional redress. If the Bureau determines, in its sole discretion, that additional redress is wholly or partially impracticable or otherwise inappropriate, or if funds remain after the additional redress

is completed, the Bureau will deposit any remaining funds in the U.S. Treasury as disgorgement. Respondent will have no right to challenge any actions that the Bureau or its representatives may take under this Section.

56. Respondent may not condition the payment of any redress to any Affected Consumer under this Order on that Affected Consumer waiving any right.

IX Order to Pay Civil Money Penalties

IT IS FURTHER ORDERED that:

57. 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, and taking into account the factors in 12 U.S.C. § 5565(c)(3), Respondent must pay a civil money penalty of \$100 million to the Bureau.

58. 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.

59. 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).

60. 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.

61. To preserve the deterrent effect of any civil money penalty in the California Enforcement Action or 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 California Enforcement Action or any Related Consumer Action because of the civil money penalty paid in this action (Penalty Offset). If the court in the California Enforcement Action or any Related Consumer Action grants such a Penalty Offset, Respondent must, within 30 days after entry of a final order granting the Penalty Offset, notify the Bureau, and pay the amount of the Penalty Offset 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.

X Additional Monetary Provisions

IT IS FURTHER ORDERED that:

62. 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.

63. 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.

64. 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.

65. Within 30 days of the entry of a final judgment, consent order, or settlement in the California Enforcement Action or any Related Consumer Action, Respondent must notify the Regional 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.

XI Reporting Requirements

IT IS FURTHER ORDERED that:

66. 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.

67. Within 7 days of the Effective Date, Respondent must designate at least one telephone number and email, physical, and postal address as points of contact, which the Bureau may use to communicate with Respondent.

68. Respondent must report any change in the information required to be submitted under Paragraph 67 at least 30 days before the change or as soon as practicable after the learning about the change, whichever is sooner.

69. Within 90 days of the Effective Date, and again at least semi-annually until the actions under this Consent Order have been completed, Respondent must submit to the Regional Director an accurate written compliance progress report (Compliance Report) that has been approved by the Board or a committee thereof, which, at a minimum:

- a. describes in detail the manner and form in which Respondent has complied with this Order;
- b. separately lists each corrective action required by this Consent Order, the Compliance Plan, and the Redress Plan;
- c. Describes the current status of each corrective action taken and the required, actual, and anticipated completion date for each corrective action; and
- d. attaches a copy of each Order Acknowledgment obtained under Section XII, unless previously submitted to the Bureau.

XII Order Distribution and Acknowledgment

IT IS FURTHER ORDERED that,

70. 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, or other agents and representatives who have responsibilities related to the subject matter of the Consent Order.

71. 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 XI, any future board members and executive officers, as well as to any managers, employees, or other agents and representatives who will have responsibilities related to the subject matter of this Consent Order before they assume their responsibilities.

72. 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.

XIII Recordkeeping

IT IS FURTHER ORDERED that

73. Respondent must create or, if already created, 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. all documents and records pertaining to the Redress Plan, described in Section VIII above.

74. Respondent must retain the documents identified in Paragraph 73 for the duration of the Consent Order.

75. Respondent must make the documents identified in Paragraph 73 available to the Bureau upon the Bureau's request.

XIV
Notices

IT IS FURTHER ORDERED that:

76. 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 Wells Fargo Bank, N.A., File No. 2016-CFPB-0015,” and send them as follows:

- a. via email to WestRegion@cfpb.gov; and
- b. via overnight courier (not the U.S. Postal Service) as follows:

Regional Director, CFPB West Region, 301 Howard Street, 12th Floor, San Francisco, CA 94105.

XV
Cooperation with the Bureau

IT IS FURTHER ORDERED that:

77. Respondent must cooperate fully to help the Bureau determine the identity and location of, and the amount of injury sustained by, each Affected Consumer. Respondent must provide such information in its or its agents’ possession or control within 14 days of receiving a written request from the Bureau.

78. Respondent must cooperate fully 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 and Respondent must cause Respondent’s officers, employees, representatives, or agents to appear for interviews, discovery, hearings, trials, and any other proceedings that the Bureau may reasonably request upon 5 days written notice, or other reasonable

notice, at such places and times as the Bureau may designate, without the service of compulsory process.

XVI Compliance Monitoring

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

79. 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.

80. 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.

81. 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.

XVII Modifications to Non-Material Requirements

IT IS FURTHER ORDERED that:

82. 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 Regional Director.

83. The Regional 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 that good cause justifies the modification. Any such modification by the Regional Director must be in writing.

XVIII

Administrative Provisions

84. 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 85.

85. 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 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.

86. This Consent Order is intended to be, and will be construed as, a final Consent Order issued under § 1053 of the CFPB, 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.

87. 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 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.

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

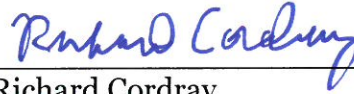
89. Should Respondent seek to transfer or assign all or part of its operations that are subject to this Consent Order, Respondent must, as a condition of sale, obtain the written agreement of the transferee or assignee to comply with all applicable provisions of this Consent Order.

90. The provisions of this Consent Order will be enforceable by the Bureau. For any violation of this Consent Order, the Bureau may seek to 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.

91. 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.

92. 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 4th day of September, 2016.



Richard Cordray
Director
Consumer Financial Protection Bureau