UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

FICARE FEDERAL CREDIT UNION,

Plaintiff, Case No. _____

v.

FISERV SOLUTIONS, LLC f/k/a
FISERV SOLUTIONS, INC., and
FISERV, INC.,

Defendants.
_____/

COMPLAINT AND DEMAND FOR JURY TRIAL;
DECLARATORY RELIEF REQUESTED; AND
PRELIMINARY AND PERMANENT INJUNCTIVE RELIEF REQUESTED

Plaintiff FiCare Federal Credit Union ("**FiCare Federal**"), sues defendants Fiserv Solutions, LLC f/k/a Fiserv Solutions, Inc. ("**Fiserv Solutions**") and Fiserv, Inc. (collectively, "**Fiserv**") and alleges:

Preliminary Statement

1. Fiserv's online banking platform, Virtual Branch Next, is insecure. It has been repeatedly hacked, again and again. FiCare Federal, a not-for-profit credit union, is one of the financial institutions using this platform. FiCare Federal's members have suffered hundreds of thousands of dollars in fraud losses because of the repeated hacks. FiCare Federal reimbursed its members to make them whole. Fiserv did not. All along, Fiserv has been on notice that

Virtual Branch Next and multiple other systems are insecure, yet Fiserv refuses to implement basic security safeguards required by its contract and federal standards. FiCare Federal brings this lawsuit to recover for the damage already done and to prevent the next hack before it occurs.

2. Fiserv sold itself to FiCare Federal as a trusted custodian of the most sensitive data a financial institution can hold: consumers' transaction histories, account numbers, and personal information. Under its Master Agreement, Fiserv promised to protect that data with the same high-tech safeguards it uses for its own information and in full compliance with federal cybersecurity standards.

3. That promise was not fulfilled. In practice, Fiserv delivered and operated systems so insecure that no financial institution should be forced to run consumer data through them. Fiserv's systems lack basic security controls. They expose member information to easy compromise. They allow hackers to easily steal staggering amounts from financial institutions. And Fiserv continued to sell and operate these systems while assuring FiCare Federal that everything was secure.

4. Fiserv's double standard makes the breach unmistakable. For its own corporate data, Fiserv deploys layered, possession-based multi-factor authentication ("**MFA**"), token generators, and biometric controls. For FiCare Federal's systems, Fiserv withheld those protections. Instead, it relied on

authentication methods so weak and susceptible to hacking that federal standards expressly prohibit their use.

5. FiCare Federal cannot fix these security failures on its own. Fiserv controls the systems that store and process FiCare Federal's data. As long as those systems remain inadequately secured, FiCare Federal faces ongoing hacking risks. Each day that passes without proper controls compounds that risk.

6. Meanwhile, Fiserv does not take security seriously. Fiserv has responded that FiCare Federal's "demand letters have imposed significant cost and inconvenience on Fiserv."

7. Fiserv has converted its own security failures into an upsell opportunity. If FiCare Federal moves to a safer service provider, Fiserv would demand seven-figure "early termination" and deconversion fees as the price of release. Fiserv's ultimatum is clear: pay the ransom, or leave data exposed on systems Fiserv refuses to secure.

8. Staying offers no refuge. Acknowledging its own deficiencies, Fiserv announced that it will discontinue its existing "Enhanced Authentication" or "Intelligent Authentication" product and force credit unions to purchase an upgrade marketed as "SecureNow," supposedly to provide additional security.

9. SecureNow does not solve the problem. It is insecure. It does not comply with federal standards for MFA. It falls far below the standard Fiserv

uses to protect its own corporate data. And SecureNow does not address the myriad of other Fiserv systems that are insecure. So, even after paying for the upgrade to SecureNow, a financial institution remains exposed to hacking risks.

10. In sum, Fiserv has attempted to monetize its own security failures by forcing credit unions to choose between paying to escape unsafe systems or paying again for security services that do not provide proper protection.

11. This is Fiserv's business model. According to *The Wall Street Journal,* Fiserv's misconduct is part of a pattern of victimizing small financial institutions and the consumers they serve. After decades of acquiring other technology providers, Fiserv now dominates the market. Fiserv's strategy is to buy up its smaller competitors to stymie competition. Meanwhile, Fiserv ceases to make the proper financial investments to keep up with emerging technology and security risks—while attempting to lock financial institutions into long-term contracts, attempting to intimidate and silence its customers from disclosing to other affected customers when there are security problems, and holding customers' data hostage when those customers seek to go to competitors. This gambit has fattened Fiserv's profits but exploited small financial institutions and the customers they serve. *See* "Frustrated by the Tech Industry, Small Banks Start to Rebel," *The Wall Street Journal,* April 11, 2019, https://www.wsj.com/articles/small-banks-rebel-against-the-most-important-

tech-firms-you-have-never-heard-of-11554975000. **Exhibit 1** is a true and correct copy of *The Wall Street Journal* article.

12. FiCare Federal brings this action to recover damages and to obtain declaratory and equitable relief that blocks Fiserv's improper charges and protects FiCare Federal's members from further hacks.

Parties

13. Plaintiff FiCare Federal Credit Union, formerly known as St. Joseph's Hospital Federal Credit Union, is a federally chartered, not-for-profit credit union with a principal place of business and localized activities in Florida. FiCare Federal has a principal place of business at 300 Jeffords Street, Clearwater, Florida.

14. Upon information and belief, defendant Fiserv Solutions, LLC, formerly known as Fiserv Solutions, Inc., is a limited liability company organized under the laws of Wisconsin, with a principal place of business at 600 N. Vel R. Phillips Avenue, Milwaukee, WI 53203. Upon information and belief, Fiserv Solutions is a wholly owned subsidiary of Fiserv, Inc.

15. Upon information and belief, defendant Fiserv, Inc. is a corporation incorporated under the laws of Wisconsin, with a principal place of business at 600 N. Vel R. Phillips Avenue, Milwaukee, WI 53203.

16. At all relevant times, each defendant acted as the agent of the other defendant and within the scope of that agency. Each defendant acted with the other defendant's authority, knowledge, consent, and ratification of the acts and omissions alleged in this Complaint.

Jurisdiction & Venue

17. This Court has original subject-matter jurisdiction over FiCare Federal's Defend Trade Secrets Act claim under 28 U.S.C. § 1331 (federal question) because it arises under the laws of the United States. Further, this Court has supplemental jurisdiction over FiCare Federal's state-law claims under 28 U.S.C. § 1367(a) because these claims are so related to the claims in the action within such original jurisdiction that they form part of the same case or controversy under Article III of the United States Constitution.

18. This Court also has subject-matter jurisdiction over FiCare Federal's claims under 28 U.S.C. § 1332 (diversity) because there is complete diversity of citizenship among the parties given that FiCare Federal is a citizen of a different state than either defendant, and the amount in controversy exceeds $75,000, exclusive of interest and costs.

19. Venue in this district is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the misconduct occurred in this district, and a substantial part of the property that is the subject of the action is situated in this district.

20. This Court has personal jurisdiction over Fiserv because Fiserv operates in this district and/or has contacts with this jurisdiction sufficient to subject it to personal jurisdiction.

Factual Background

21. FiCare Federal is a not-for-profit cooperative owned by individual consumers, who pool their resources to provide credit to one another. Founded in 1960, FiCare Federal serves members who work in the healthcare industry. FiCare Federal offers a range of financial services, including savings accounts, checking accounts, loans, and online banking.

22. Fiserv is among the largest technology vendors to credit unions and banks. It claims approximately 10,000 financial institution clients and provides technology to more than one in three U.S. financial institutions.

23. FiCare Federal contracted with Fiserv to provide technology services under a Master Agreement. **Exhibit 2** is a true and correct copy of the Master Agreement, as amended.

24. Among the services Fiserv provides are account processing services. An account processing system is the "brains" behind a financial institution, processing and recording all transactions for the financial institution.

25. Fiserv stores and processes FiCare Federal's most sensitive information, including member names, account numbers, balances, transaction

histories, and other personally identifying information, across various Fiserv systems.

26. **Contractual Standard of Care.** Under the Master Agreement, Fiserv was required to follow the following standards of care:

a. Section 3(b) of the Master Agreement requires Fiserv to "use the same care and discretion to avoid disclosure of Information as it uses with its own similar information that it does not wish disclosed, but in no event less than a reasonable standard of care and no less than is required by law." (Exhibit 2 at § 3(b).)

b. Section 4(a) of the Master Agreement requires Fiserv to implement and maintain an information security program that is designed to meet the following objectives:

i. "protect the security and confidentiality of customer information";

ii. "protect against any anticipated threats or hazards to the security or integrity of such information";

iii. "protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer"; and

iv. "ensure the proper disposal of 'consumer information'."

(Exhibit 2 at § 4(a).)

c. The Virtual Branch Services Schedule to the ASP Services Exhibit requires Fiserv to provide "Enhanced Authentication," beyond a baseline level of minimally acceptable authentication.

27. Fiserv protects its own confidential data with robust, high-assurance measures, including token-generated codes, biometric identifiers, and other layered authentication controls, in addition to phishing-resistant multi-factor authentication.

28. **What FiCare Federal Received.** Despite these contractual obligations, Fiserv failed to implement these protections for FiCare Federal's confidential information. Instead, Fiserv deployed materially weaker controls, leading to repeated hacks of FiCare Federal accounts.

29. **Why MFA Matters.** MFA is an additional security control that counters the most common hacking vector, a compromised password, by requiring two or more distinct factors: something the user knows (such as a password), possesses (such as a device or token), or is (such as biometric verification). MFA makes an account 99% less likely to be hacked.[1]

[1] https://www.cisa.gov/topics/cybersecurity-best-practices/multifactor-authentication

30. Not all MFA is created equal. Some forms, such as codes sent by email or text, do not establish possession of a particular device. Those forms provide inadequate security because they are susceptible to hacking by interception, SIM-swap, or account takeover.

31. Federal standards and supervisory guidance reinforce these differences. The Federal Financial Institutions Examination Council's *Authentication and Access to Financial Institution Services and Systems*[2] adopts the *Digital Identity Guidelines* of the National Institute of Standards and Technology ("**NIST**"), which mandates: "Methods that do not prove possession of a specific device, such as … email, SHALL NOT be used for out-of-band authentication." *See* NIST SP 800-63B § 5.1.3.1.[3] This further requires that "[i]n the absence of a trusted statement that it is a multi-factor device, the verifier SHALL treat the authenticator as single-factor." *Id.* § 5.1.5.2.

32. A July 2025 update to NIST's *Digital Identity Guidelines* reinforces that codes sent by email are insufficient to provide proper MFA: "Email SHALL NOT be used for out-of-band authentication because it may be vulnerable to:

- Access using only a password

[2] https://www.ffiec.gov/sites/default/files/media/press-releases/2021/authentication-and-access-to-financial-institution-services-and-systems.pdf

[3] https://pages.nist.gov/800-63-3/sp800-63b.html

- Interception in transit or at intermediate mail servers
- Rerouting attacks, such as those caused by Domain Name System (DNS) spoofing."[4]

33. Codes sent by text message are insecure. The United States Cybersecurity and Infrastructure Security Agency describes text message codes as a "last resort MFA option" and appropriate only as a "temporary solution when organizations transition to a stronger MFA implementation."[5] This is because it is fairly simple to intercept or redirect text messages, so a text message code is insufficient to satisfy the "what you have" factor by establishing possession of a particular device.

34. On at least one system housing FiCare Federal's confidential information, Fiserv has not required any MFA or email passcode challenge at all.

35. For other systems housing FiCare Federal's confidential information, Fiserv relied on an email passcode challenge instead of MFA. Email does not establish possession of a specific device and does not qualify as a second factor under federal regulatory guidance. Nor does Fiserv use this weak method to

[4] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63B-4.pdf

[5] https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

secure its own confidential information. It therefore fails to meet the standard of care Fiserv owes under the Master Agreement.

36. On other access paths, Fiserv uses codes sent over text message. Text message codes are insufficient to satisfy the possession factor of MFA. At best, as the above federal regulatory guidance explains, text message codes are a temporary bridge to stronger, phishing-resistant MFA. Fiserv deploys stronger possession-based MFA such as token- or app-based authenticators to protect Fiserv's own confidential information, but fails to provide equivalent protections to FiCare Federal. This breaches the Master Agreement.

37. Fiserv's failure to deploy promised safeguards has resulted in FiCare Federal being hacked repeatedly, as well as FiCare Federal paying for services that were not properly performed. Meanwhile, Fiserv has materially increased the risk of further hacking and unauthorized access to FiCare Federal's extraordinarily sensitive confidential information.

Fiserv's Pattern:
Known Security Gaps, False Assurances, and Active Concealment

38. Fiserv has long known that the authentication controls on its systems sold to financial institutions suffer from serious security defects. Yet Fiserv continued to sell, deliver, and operate those platforms while assuring financial-institution clients that their systems and data remained secure. Fiserv's knowing and willful misconduct—a combination of knowledge of security

problems, false assurances its systems had certain security controls, and concealing the absence of security controls—amounts to fraud.

39. Fiserv received repeated warnings that its controls failed to protect financial institutions. Instead of fixing root causes, Fiserv relied on outdated practices and patchwork responses. Those choices exposed FiCare Federal's member information to compromise by hackers and forced FiCare Federal—and other institutions—to operate under hidden, avoidable risk.

40. In August 2018, *Krebs on Security* reported a Fiserv defect that allowed unauthorized access to consumers' account and transaction records and allowed changes to phone numbers and email addresses used for transaction alerts.[6]

41. Customers attempted to alert Fiserv. Yet Fiserv did not treat the defect as urgent. Fiserv acted only after media scrutiny made inaction reputationally costly.

42. Despite customer efforts to notify Fiserv directly (including messages sent to the social media accounts of Fiserv's CEO and various other individuals who were identified as affiliated with Fiserv), Fiserv ignored these warnings until media scrutiny compelled it to implement a fix.

---

[6] "Fiserv Flaw Exposed Customer Data at Hundreds of Banks," https://krebsonsecurity.com/2018/08/fiserv-flaw-exposed-customer-data-at-hundreds-of-banks/.

43. Fiserv spokesperson Ann Cave admitted publicly that Fiserv delayed addressing these known problems until media exposure forced its hand, confirming its reckless disregard for customer security. Ms. Cave confirmed that Fiserv did not make efforts to remediate this known threat until ***after*** receiving an inquiry from a ***reporter***—when negative press coverage was imminent. According to Ms. Cave, "[a]fter receiving [the reporter's] email, [Fiserv] promptly engaged appropriate resources and worked around the clock to research and remediate the situation. [Fiserv] developed a security patch within 24 hours of receiving notification and deployed the patch to clients that utilize a hosted version of the solution. [Fiserv] will be deploying the patch this evening to clients that utilize an in-house version of the solution." Thus, only after Fiserv faced the imminent prospect of negative press attention did Fiserv "promptly engage[] appropriate resources" to fix its security lapse. This delay, however, left hundreds of financial institutions vulnerable long after Fiserv knew of the risk.

44. Fiserv's lackadaisical approach to cybersecurity persists to this day.

45. Unfortunately, Fiserv's corporate culture discouraged emphasis on data security. For example, even one of Fiserv's own employees recognized the inadequacy of Fiserv's support and outreach channels. In a post responding to another *Krebs on Security* article about additional security problems with Fiserv's online banking platform, Adam Kinder, Fiserv's Information Security Manager,

publicly invited customers to message him through his personal social media account[7] so that he "can use what influence [and] means I have at our company, above and beyond customer support and outreach branches, to address their concerns." That public admission tracks what Fiserv's customers experienced: Fiserv's formal channels did not reliably surface or remediate high-risk security defects.

46. For Fiserv, serious efforts at compliance often begin at the proverbial courthouse steps. When regulated financial institutions demand that Fiserv honor its security and oversight obligations, Fiserv resists until litigation forces the issue and compels action. Public filings reflect that pattern.

[7] Fiserv's Code of Conduct & Business Ethics, which was in effect at or around the time of Kinder's comment, contains a social media policy that covers the use of LinkedIn, Twitter, Facebook, forums, and blogs, and Fiserv regulates its employees' use of Fiserv's trademarks on social media. Fiserv notes that social media "is an established part of many people's personal and professional lives-and the lines have blurred." *See* https://web.archive.org/web/20230601125645/https://investors.fiserv.com/static-files/2cef514b-b67b-45c7-9aaa-70ccedbdb25c. The current version of Fiserv's Code of Conduct & Business Ethics, which contains the same social media policy is available at https://d1io3yog0oux5.cloudfront.net/_583f477852403c9df0b7b630e3701167/fiserv/db/2275/21421/file/Code+of+Conduct+%26+Business+Ethics.pdf. Accordingly, Fiserv knows, or should have known, about communications sent to the social media accounts of its agents who have identified themselves as Fiserv representatives on social media platforms.

47. In 2022, the U.S. Courthouse SDNY Federal Credit Union, the credit union serving judges and employees of the U.S. District Court for the Southern District of New York, sued Fiserv over online-banking security failures and to challenge Fiserv's asserted early-termination fee when that credit union was seeking to exit Fiserv while undergoing a merger with another credit union. *U.S. Courthouse SDNY Federal Credit Union et al. v. Fiserv Solutions, LLC et al.*, No. 1:22-cv-09329 (S.D.N.Y. 2022). Fiserv resolved the case shortly after it was filed.

48. Other litigation raising security concerns includes *Bessemer System Federal Credit Union v. Fiserv Solutions, LLC et al.*, No. 2:19-cv-00624-RJC (W.D. Pa. 2019), *Cencap Federal Credit Union v. Fiserv Solutions, LLC*, Case No. 3:25-cv-00913-VDO (D. Conn. 2025), and *Self-Help Credit Union v. Fiserv Solutions, LLC*, Case No. 1:25-cv-01112-TDS-LPA (M.D.N.C. 2025).

49. Instead of candidly disclosing known defects to its clients and coordinating remediation, Fiserv actively concealed defects from becoming known to its clients. When another credit union reported security problems that allowed online banking accounts to be readily taken over by hackers, Fiserv responded with threats and litigation pressure designed to silence disclosure. Indeed, Fiserv demanded that the credit union "[r]efrain from dissemination or disclosure of any information or records relating to the 'security review' to third

parties, including any clients…of Fiserv." Those threats and misconduct did not protect Fiserv's customers; it protected Fiserv's reputation and revenue.

Fiserv's "Sunset" Play: Remove Security Features Mid-Contract, Then Sell Those Features Back as "SecureNow" with Additional Pricing

50. Fiserv puts revenue first. On December 18, 2025, it sent its credit union customers an "Enhanced Authentication Product Sunset Notice." The notice stated that Fiserv would discontinue the existing "Enhanced Authentication" feature for Virtual Branch Next effective May 31, 2026.

51. "Enhanced Authentication" is a lie: as shown above, Fiserv has not even provided baseline authentication for FiCare Federal, much less any "advanced" authentication.

52. Fiserv paired the withdrawal of Enhanced Authentication with a sales deadline. Fiserv's notice said that credit unions must sign a new agreement by March 2, 2026 to receive a replacement service Fiserv markets as "SecureNow," which Fiserv touts as "additional security" for Virtual Branch Next.

53. SecureNow is not an "upgrade." It is a mid-contract shake-down. Fiserv already owes FiCare Federal and its other customers a contractual duty to safeguard their confidential information. Fiserv cannot pull back security features mid-contract and then sell them back under new terms and higher pricing.

54. SecureNow does not solve the problem it claims to address. The name sounds reassuring; its functionality is not. SecureNow does not provide possession-based MFA and therefore fails to address the root cause of online banking account takeovers. In short, even a credit union that pays for SecureNow remains exposed to hackers and still cannot meet evolving regulatory expectations for protecting member information.

Fiserv Defrauds Its Financial Institution Customers, Including FiCare Federal

1. Fiserv Provides a Fraudulent "Compliance Package" to Financial Institutions Misrepresenting the Security Controls Fiserv Has on Its Systems

55. As a regulated financial institution, FiCare Federal must conduct oversight of third-party vendors such as Fiserv. To facilitate and influence that oversight, Fiserv provides its financial-institution customers with a "Compliance Package" that represents Fiserv has implemented security measures to meet financial-institution regulatory requirements.

56. Fiserv updates its compliance package from time to time and assures FiCare Federal that Fiserv continues to comply with evolving regulatory and industry requirements. The representations in Fiserv's compliance package were false and misleading.

57. Among the materials in Fiserv's compliance package is Fiserv's *Standard Information Gathering Questionnaire*. FiCare Federal and other Fiserv

customers use this questionnaire to assess Fiserv's security posture and vendor risk.

58. The questionnaire asks: "Are policies and standards based on accepted control standards, frameworks, and industry practices?"

59. Fiserv answered "Yes," and further represented that Fiserv's cybersecurity policies and standards track NIST and other recognized standards. Specifically, Fiserv represented, among other things:

> Fiserv has established a Global Cybersecurity and Technology Management Policy based on NIST's CSF (National Institute of Standards and Technology, Cyber Security Framework) which is a subset of controls within the comprehensive NIST SP 800-53 standard. The Global Cybersecurity and Technology Management Policy and standards have been designed to meet applicable industry and regulatory requirements.
>
> - Interagency Guidelines Establishing Information Security Standards and on Response Programs for Unauthorized Access to Customer Information and Customer Notice
> - EU General Data Protection Regulation (GDPR)
> - Applicable European Banking Authority (EBA) guidelines
> - Fair Credit Reporting Act (FCRA)
> - Gramm-Leach-Bliley Act (GLBA)
> - Health Insurance Portability and Accountability Act (HIPAA)
> - Numerous state and /or country specific privacy and security laws including the IT Security Act 2.0 from the German Federal Office for Information Security
> - International Organization for Standardization (ISO) 27001, Information Security Management

- National Institute of Standards and Technology (NIST) Cyber Security Framework
- Payment Card Industry Data Security Standard (PCI DSS)

60. Those statements were false and misleading. As described above, Fiserv did not comply with accepted control standards, frameworks, and industry practices, including NIST authentication requirements.

61. The questionnaire also asks: "Is Multi-Factor Authentication (MFA) utilized?" Fiserv answered: "Yes."

62. That statement was false and misleading. As described above, Fiserv did not utilize MFA on at least one of its systems, and the authentication process used does not meet recognized standards for MFA.

63. Fiserv also provided FiCare Federal with a *Fiserv Cybersecurity Fact Sheet 2025*, which again represented that "Fiserv has established a Global Cybersecurity and Technology Management Policy based on authoritative sources that include regulatory and industry publications such as NIST's CSF (National Institute of Standards and Technology, Cyber Security Framework) which is a subset of controls within the comprehensive NIST SP 800-53 standard."

64. The *Fiserv Cybersecurity Fact Sheet 2025* further represented that Fiserv's policy and standards "have been designed to meet applicable industry

and regulatory requirements," including NIST's "Cyber Security Framework, 800-53, 800-63-3."

65. Those statements were false and misleading. As set forth above, Fiserv's use of an "email passcode challenge" as a purported second factor for MFA violates NIST Special Publication 800-63-3, which expressly prohibits email from being used for MFA.

2. Fiserv Publishes a False and Misleading Privacy Notice

66. Fiserv, Inc. publishes a publicly available "Privacy Notice" that states, as present fact, the security measures Fiserv claims it has in place to protect customer data. The Privacy Notice purports to apply to Fiserv, Inc. and all subsidiaries and affiliates, including Fiserv Solutions.[8]

67. In Section 6, Fiserv represents: it has "in place appropriate security measures to prevent…personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed."

68. That statement was false and misleading when made. Contrary to Fiserv's representation, Fiserv did not have appropriate security measures in place to prevent FiCare Federal's data from being used or accessed in an unauthorized way.

[8] A copy appears at https://www.fiserv.com/en/about-fiserv/privacy-notice.html.

69. Fiserv's misrepresentations and concealments harmed FiCare Federal in a straightforward way: it deprived FiCare Federal of material facts that would have altered FiCare Federal's decisions about risk, vendor oversight, and continued use of Fiserv services. Fiserv withheld the truth while continuing to accept payment for services it represented as secure and compliant with contractual and legal requirements.

70. Fiserv had strong financial motives to sustain the appearance of robust cybersecurity to maintain market and customer confidence in its systems. Fiserv's public filings reflect that goodwill and intangible assets comprise a significant portion of Fiserv's corporate assets, and as a publicly traded company, Fiserv's valuation depends on market and customer confidence in its systems. By suppressing adverse security information and downplaying risk, Fiserv misleadingly obtained customer revenue, reduced its customers' switching pressure, and fattened corporate goodwill—at its customers' expense.

71. Fiserv's incentives to deceive intensified recently as Fiserv's share price fell sharply. Fiserv's stock is down approximately 70% over the past year, heightening Fiserv's pressure to avoid disclosures that could further impair market confidence and customer retention.

72. Fiserv's misconduct was far from accidental. Fiserv knew about material security defects, minimized or misrepresented them, delayed

remediation until external exposure threatened, and pressed to suppress the truth from its customers.

73. That course of conduct shows willful, wanton, and reckless disregard for the privacy and security of financial-institution customers and their members and supports an award of punitive damages.

74. As a direct result, FiCare Federal has incurred and will continue to incur substantial costs to protect members, monitor for fraud, investigate suspicious activity, reimburse members' fraud losses, and mitigate long-tail identity-theft risks created by Fiserv's security failures.

The Severe Impact on FiCare Federal and Its Members

75. The information entrusted to Fiserv includes highly sensitive personal and financial data. If compromised, identity thieves can weaponize that data to drain accounts, change contact credentials, defeat fraud alerts, and impersonate members across other systems.

76. The harm does not end with a single incident. Once exposed, member information can circulate indefinitely, including through illicit marketplaces. Members face continuing risk of identity theft, account takeover, and downstream fraud—often months or years after the original exposure.

77. Cybercriminals also exploit stolen data to inflict non-monetary harms, including harassment, extortion attempts, and targeted stalking.

Transaction times and locations can reveal personal routines and physical whereabouts.

78. Most importantly, members face irreparable harm when hackers gain access to their most sensitive financial information. Transactional data can reveal intimate facts of members' lives, including, for example, which members paid retainers to a divorce attorney or which members received care from a psychiatrist, drug-rehabilitation clinic, cancer center, fertility clinic, or abortion clinic.

79. Public reporting has recognized the hidden emotional toll of data breaches, a unique form of irreparable harm. While some victims report direct financial impacts, many more—50%—report emotional harm. Nearly one-third said a breach had affected their physical well-being, and nearly a quarter said their relationships were personally affected. Data breaches can expose diagnoses, medical procedures, and other highly sensitive personal information while leaving victims living with persistent anxiety: when will criminals use my data, and how? *See* "The Hidden Emotional Toll on Victims of Data Breaches," *The Wall Street Journal*, Nov. 25, 2025, https://www.wsj.com/tech/cybersecurity/data-breach-victims-0b01a5ab?mod=Searchresults&pos=2&page=1. **Exhibit 3** is a true and correct copy of *The Wall Street Journal* article.

80. Criminals can also use FiCare Federal's member information to fuel embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud, including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. For example, the times and locations members use their debit cards can be used to stalk and victimize those individuals. A report from the United States Government Task Force on Identity Theft explains the harm to FiCare Federal:

> Businesses suffer most of the direct losses from ... identity theft because individual victims generally are not held responsible for fraudulent charges. Individual victims, however, also collectively spend billions of dollars recovering from the effects of the crime.
>
> In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, monetary costs of identity theft include indirect costs to businesses for fraud prevention and mitigation of the harm once it has occurred (e.g., for mailing notices to consumers and upgrading systems). Similarly, individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit....
>
> In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their

> reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.[9]

81. To put it into context, the FBI Internet Crime Complaint Center's 2024 Internet Crime Report reveals that, between 2020 and 2024, it received 4.2 million complaints related to various internet scams impacting American citizens around the globe, amounting to a staggering $50.5 billion in reported losses, and an average of 836,000 complaints received per year. In 2024 alone, the crime categories of personal data breach, general data breach, credit card/check fraud, and identity theft accounted for $2.19 billion in losses. The average reported loss per complaint in 2024 was $19,372.[10]

82. Stolen data can also be offered for sale on the "dark web," a heavily encrypted part of the internet that makes it difficult for authorities to detect a website's location or owners. The dark web is not indexed by normal search engines such as Google and is accessible only by using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling items such as weapons, drugs, and

---

[9] The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Federal Trade Commission, 11 (April 2007).

[10] *See* https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

personal information. Sites on the dark web appear and disappear quickly, providing cover for illegal transactions.

83. Once a bad actor buys member information, it can then be used to gain access to different areas of the victim's digital life, including financial accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

84. In addition to member information that can be accessed, a hacked online banking account can be very valuable to cyber criminals for other attacks. Since online banking accounts are linked to other accounts (for example, to transfer funds between financial institutions), a hacked online banking account can serve as a gateway for additional criminal activity.

85. The problems associated with identity theft are exacerbated by the fact that many identity thieves will delay exploiting stolen information, extending the threat of identity theft long after the initial breach. The stolen data may be listed for sale on the dark web years after the initial breach, enabling unauthorized individuals to purchase and exploit it after the security incident has faded from immediate concern.

86. Compounding this risk is the practice known as "dwell" by hackers, where unauthorized access remains undetected for extended periods, amplifying

long-term harm. During this time, cybercriminals can continue exploiting access across multiple systems within the same network, gather additional sensitive information, and fortify their control over compromised data without triggering immediate detection. This latency often results in the hack going unnoticed until long after the initial breach, amplifying the potential for further exploitation.

87. Because hackers can remain undetected for extended periods and delay the use of stolen information, the full scope of the breach may not be immediately apparent. Indeed, in order to protect its member information, FiCare Federal will need to remain vigilant against compromise and unauthorized use of its member information for years and decades to come.

FiCare Federal Repeatedly Reports Deficiencies in Fiserv's Security; Fiserv Fails to Fix the Problems

88. Unfortunately, FiCare Federal and its members have first-hand experience with the risks created by Fiserv's deficient security infrastructure. In 2024, a hacker obtained control over online banking accounts during FiCare Federal's Virtual Branch account creation process, resulting in substantial losses to FiCare Federal.

89. FiCare Federal gave Fiserv notice of the hacker's specific breaches of the security systems in place, but Fiserv failed to take any action to properly secure FiCare Federal's information and systems, including failing to implement MFA as required by federal regulations.

90. The losses resulting from Fiserv's cavalier approach to combating known threats to FiCare Federal's systems continues unabated

91. In addition, FiCare Federal has identified other problems with Fiserv's performance and submitted support tickets to Fiserv which have gone unremedied.

92. Given the ongoing security risks, and Fiserv's refusal to deal with them in a timely manner, FiCare Federal sent Fiserv a Notice of Breach on or about July 3, 2025.

93. In addition to notifying Fiserv of its breaches of the Master Agreement and demanding that those breaches be remedied, FiCare Federal also exercised its right under the Master Agreement for information concerning Fiserv's performance (or lack thereof). Specifically, FiCare Federal's requests included:

a. Copies of audits, summaries of test results, and other equivalent evaluations of Fiserv's security, as required by § 4(a) of the Master Agreement and 12 C.F.R. Part 748, Appendix A;

b. A summary of Fiserv's written information security plan for the services provided to FiCare Federal within 30 days, as required by § 4(b) of the Master Agreement;

c. Documentation supporting the amounts invoiced by Fiserv for the 12-month period prior to the date of the Notice of Breach, as required § 10(b) of the Master Agreement;

d. Copies of Fiserv's most recent security certifications for the service centers providing services to FiCare Federal, as required by § 4(d) of the ASP Services Exhibit to the Master Agreement;

e. Copies of the independent audit reports of the Fiserv service centers providing service to FiCare Federal, as required by § 4(h) of the ASP Services Exhibit to the Master Agreement; and

f. Results of Fiserv's tests of its Disaster Recovery Plan, as required by § 6(c) of the ASP Services Exhibit to the Master Agreement.

94. Fiserv did not produce the summary of its information security plan until August 28, 2025 (nearly 60 days after FiCare Federal's request).

95. Furthermore, by letter dated August 29, 2025, Fiserv rejected FiCare Federal's request for documentation supporting Fiserv's invoices as "unreasonable" because FiCare Federal did not identify the specific services FiCare Federal believed it was improperly charged for, even though no such requirement appears in the Master Agreement.

96. Fiserv's August 29, 2025 response also claimed that the remainder of the documents requested "will be provided in due course."

97. To date, no such documents have been produced by Fiserv, in breach of its audit obligations.

FiCare Federal's Claims Are Timely, as Both the Statute of Limitations and Contractual Limitations Period Have Been Tolled

98. FiCare Federal exercised reasonable diligence but could not discover Fiserv's misconduct earlier due to Fiserv's deliberate and active concealment.[11]

99. FiCare Federal became aware of the harm caused by Fiserv's security deficiencies only recently, well within the applicable limitations period.

100. FiCare Federal previously did not suspect, and had no reason to suspect, that Fiserv's products and services caused damages and harm.

101. The highly technical nature of Fiserv's products and services prevented earlier detection of these serious cybersecurity problems.

102. Fiserv maintained exclusive knowledge of the material defects and vulnerabilities designed and implemented into its products and services, actively misleading FiCare Federal.

[11] "As the discovery rule has developed, the salient point giving rise to its application is the inability of the injured, despite the exercise of reasonable diligence, to know what he is injured and by what cause." *Bessemer Sys. Fed. Credit Union v. Fiserv Sols., LLC*, 472 F. Supp. 3d 142, 168 (W.D. Pa. 2020) (quoting *Fine v. Checcio*, 582 Pa. 253, 870 A.2d 850, 858 (Pa. 2005)) (denying Fiserv's motion to dismiss the plaintiff credit union's claim as time-barred, relying on the discovery rule).

103. In addition, Fiserv's fraudulent concealment and/or other tortious conduct has tolled the running of any statute of limitations.

104. Fiserv was actually aware of the material defects in its systems, and its failure to comply with regulatory and contractual requirements. Fiserv also knowingly, affirmatively, and actively concealed from FiCare Federal the risks associated with the defects of its products and services, and that these defects caused damages and harm to FiCare Federal.

105. Fiserv's purpose in concealing these facts was to induce FiCare Federal to continue relying on its services and to delay FiCare Federal's discovery of its claims. By concealing material information, Fiserv sought to avoid early detection of its misconduct and to prevent FiCare Federal from initiating legal action within the applicable limitations period.

106. Fiserv committed tortious and/or fraudulent acts that continue to this day. As of the date of this Complaint, Fiserv still has not disclosed, and continues to conceal, that it designed and implemented insecure features into its products and services, and that the representations it made about the security of its services are false. Despite its knowledge of the defects and their attendant risks, Fiserv continues to market its products and services to financial institutions while simultaneously omitting the disclosure of known and foreseeable harms.

107. FiCare Federal was unaware and could not have reasonably known or learned through reasonable diligence that it had been exposed to the defects and risks alleged herein and that those defects and risks were the direct and proximate result of Fiserv's acts and omissions.

108. Moreover, Fiserv's obligations under the Master Agreement are ongoing and include the continued implementation of appropriate information security measures, adherence to regulatory requirements, and the exercise of good faith and fair dealing in not exposing FiCare Federal to vastly greater harm than bargained for and well outside commercially reasonable norms. Each act of non-compliance with these contractual obligations renewed the limitations period under the continuing duty doctrine.

109. For the foregoing reasons, Fiserv is estopped from relying on any statutes of limitation or repose, or other time-based defenses in this action. All applicable statutes of limitation and repose have been tolled by operation of the discovery rule, the continuing duty doctrine, and by Fiserv's active concealment with respect to all claims against it.

First Claim for Relief
Breach of Contract
(Against Fiserv Solutions Only)

110. FiCare Federal repeats the allegations in the preceding paragraphs.

111. The Master Agreement is a valid contract binding Fiserv Solutions.

112. In addition to the express terms of the Master Agreement, the implied covenant of good faith and fair dealing applies to the Master Agreement. To vindicate the parties' apparent intentions and reasonable expectations, Fiserv Solutions was obligated to invoice only for services actually and properly performed and to provide security appropriate for a federally regulated credit union that stores extraordinarily sensitive consumer financial information.

113. FiCare Federal has duly performed all obligations and satisfied all conditions required of it under the Master Agreement, except for those that were waived or excused by Fiserv Solutions.

114. Fiserv Solutions materially breached the Master Agreement, including by:

a. violating Section 3(b) of the Master Agreement by failing to use the same care and discretion to avoid disclosure of FiCare Federal's confidential information as Fiserv uses with its own similar information that it does not wish disclosed, but in no event less than a reasonable standard of care and no less than is required by law;

b. violating Section 4(a) of the Master Agreement by failing to implement and maintain an information security program that appropriately protects the security and confidentiality of FiCare Federal's information;

c. violating Section 4(a) of the Master Agreement by failing to take appropriate actions to address incidents of unauthorized access to FiCare Federal's sensitive customer information, including by failing to notify FiCare Federal as soon as possible of those incidents;

d. violating Section 4(h) of the ASP Services Exhibit to the Master Agreement by failing to develop and implement an action plan to address and resolve material security deficiencies uncovered during audits;

e. violating Section 4(a) and 4(b) of the Master Agreement, and Sections 4(d), 4(h) and 6(c) of the ASP Services Exhibit to the Master Agreement, by failing to provide the documentation required to be produced to FiCare Federal;

f. violating Section 10(b) of the Master Agreement by refusing to provide FiCare Federal with documentation supporting the amounts invoiced by Fiserv;

a. violating the Virtual Branch Services Schedule to the ASP Services Exhibit by failing to provide, and repudiating its obligation to provide in the future, "Enhanced Authentication";

g. violating N.Y. General Obligations Law § 5-903 by purporting to effectuate an automatic renewal of the Master Agreement without

providing the required personal or certified mail notice to FiCare Federal beforehand;

h. repudiating its obligations, including by discontinuing Enhanced Authentication services mid-contract and insisting that FiCare Federal agree to additional and different contract terms and pay additional charges for "SecureNow" or other ostensible security upgrades that Fiserv is under a preexisting contractual duty to provide; and

i. violating the implied covenant of good faith and fair dealing by issuing invoices for services not properly performed and exposing FiCare Federal to hacking and fraud risks vastly greater than it had bargained for and well outside of commercially reasonable norms.

115. Fiserv Solutions' contract breaches were, at a minimum, grossly negligent. Fiserv had actual knowledge, through reports from financial institutions and others, that Fiserv's security controls were absent or woefully insecure and have led to significant fraud losses and hacking at other financial institutions. Fiserv Solutions, however, failed to properly investigate or secure its systems. Nor did Fiserv Solutions alert FiCare Federal of the security problems.

Fiserv Solutions' contract breaches smack of intentional wrongdoing and evince a reckless indifference to FiCare Federal's rights.[12]

116. Fiserv Solutions' misconduct was not an isolated incident; it is part of a dangerous pattern that put life savings and extraordinarily sensitive financial information of scores of consumers into the reach of hackers. By withholding basic safeguards from FiCare Federal's systems despite known hacking risks, Fiserv exposed thousands of consumers to hacking, fraud, and identity theft. And FiCare Federal is not alone: Fiserv's deficient approach to cybersecurity for its clients has also endangered countless other financial institutions and their customers. Fiserv's misconduct is actionable as an independent tort as well as egregious, repeated, and directed at FiCare Federal as part of a broader course of conduct that endangers the public. Fiserv's misconduct reflects a high degree of moral turpitude and such wanton dishonesty as to imply a criminal indifference to Fiserv's civil obligations.

[12] New York law governs the Master Agreement. New York public policy bars parties from contracting away liability for gross negligence, even in business-to-business contracts signed by sophisticated parties. The limitation-of-liability clause in the Master Agreement therefore offers Fiserv no protection because its failure to fulfill its obligation to secure FiCare Federal was, at a minimum, grossly negligent. In *Abacus Federal Savings Bank v. ADT Security Services, Inc.*, 967 N.E.2d 666, 670 (N.Y. 2012), New York's highest court held that a financial institution could recover full, uncapped damages from a security vendor whose gross negligence left the institution insecure. Fiserv's misconduct here is no less grave. The same principle applies, and the damages here are not subject to any contractual cap.

Punitive damages are appropriate to deter Fiserv from endangering others in the same way again. The amount of such punitive damages should be sufficient to have a deterrent effect on Fiserv, which has a market capitalization valued at over $36 Billion.

117. As a direct and proximate result of Fiserv Solutions' contract breaches, FiCare Federal has suffered and will continue to suffer damages and harm.

WHEREFORE, FiCare Federal respectfully requests that judgment be entered in its favor on Count 1 for monetary damages, rescission, restitution and disgorgement, indemnification, declaratory relief, specific performance, injunctive relief, costs of litigation (including attorneys' fees and costs), and such other and further relief to FiCare Federal as the Court deems appropriate under the circumstances.

Second Claim for Relief
Rescission of Master Agreement[13]
(Against Fiserv Solutions Only)

118. FiCare Federal repeats the allegations in the preceding paragraphs.

119. FiCare Federal is entitled to rescission of the Master Agreement due to Fiserv's breaches. The breaches are so material, willful, substantial, and

[13] As permitted by Fed. R. Civ. P. 8(a)(3), FiCare Federal is demanding different types of relief, including in the alternative, in connection with its claims.

fundamental that they have defeated the object of the parties in making the Master Agreement. These breaches have caused FiCare Federal to be repeatedly hacked and subjected to future hacks, leaving FiCare Federal in a position substantially different from what the parties intended at the time they entered into the Master Agreement.

120. FiCare Federal is entitled to rescission of the Master Agreement because Fiserv misrepresented to FiCare Federal the existence and nature of Fiserv's security controls and its intent to perform the Master Agreement. These representations were material to FiCare Federal, and it reasonably relied on them in deciding whether to enter into and continue performing under the Master Agreement, which did not disclaim reliance on these types of specific representations. The falsity of Fiserv's representations was within Fiserv's peculiar knowledge and could not have been reasonably discovered by FiCare Federal.

121. FiCare Federal is entitled to rescission of the Master Agreement due to commercial impracticability and frustration of purpose. Unforeseeable events not caused by FiCare Federal have altered the essential nature of the Master Agreement, and FiCare Federal has been unable to obtain its expected bargain from Fiserv.

122. FiCare Federal has no adequate remedy at law. Accordingly, this Court should rescind the Master Agreement.

WHEREFORE, FiCare Federal respectfully requests that judgment be entered in its favor on Count 2 for rescission, restitution and disgorgement, injunctive relief, costs of litigation (including attorneys' fees and costs), and such other and further relief to FiCare Federal as the Court deems appropriate under the circumstances.

Third Claim for Relief
Specific Performance
(Against Fiserv Solutions Only)

123. FiCare Federal repeats the allegations in the preceding paragraphs.

124. The Master Agreement is a valid contract binding Fiserv Solutions.

125. FiCare Federal has performed or substantially performed its obligations under the Master Agreement.

126. FiCare Federal is ready, willing, and able to perform its remaining obligations until the contract terminates or is rescinded by an order of this Court.

127. Fiserv Solutions is presently breaching, and absent relief will continue to breach, its contractual obligations to safeguard FiCare Federal's confidential information.

128. Fiserv Solutions has repudiated the Master Agreement, and absent relief will continue to breach the Master Agreement, by withdrawing security

offerings provided under the Master Agreement and compelling FiCare Federal to accept new service offerings (such as "SecureNow"), at increased prices, in order for Fiserv to continue performing its preexisting duty to safeguard FiCare Federal's confidential information.

129. Fiserv is capable of performing the Master Agreement, including by deploying phishing-resistant, possession-based MFA and other enhanced security controls that it uses to safeguard its own sensitive data.

130. The loss of confidentiality and risk of unauthorized access constitute irreparable harms not adequately compensable by money damages alone.

131. Accordingly, the Court should issue an order of specific performance compelling Fiserv Solutions to specifically perform its obligations to FiCare Federal, including securing FiCare Federal's confidential information as required by the Master Agreement.

WHEREFORE, FiCare Federal respectfully requests that judgment be entered in its favor on Count 3 for specific performance, injunctive relief, costs of litigation (including attorneys' fees and costs), and such other and further relief to FiCare Federal as the Court deems appropriate under the circumstances.

Fourth Claim for Relief
Declaratory Relief
(Against Fiserv Solutions Only)

132. FiCare Federal repeats the allegations in the preceding paragraphs.

133. Genuine disputes exist between the parties concerning the Master Agreement and its existence, meaning, enforceability, and applicability. There is a bona fide adverse interest and present controversy between the parties concerning FiCare Federal's rights and Fiserv Solutions's obligations.

134. FiCare Federal doubts the positions Fiserv Solutions has taken regarding FiCare Federal's rights and Fiserv's obligations.

135. FiCare Federal is entitled to have the doubts removed. This Court's declarations of the parties' rights and obligations would resolve the legal relations of the parties to justiciable controversies.

136. **No Obligation to Pay for or Contract for "SecureNow" (Preexisting Contractual Duty; Inadequate Security).** FiCare Federal seeks a declaration that it has no obligation to enter into any agreement for Fiserv's "SecureNow" service. Under the Master Agreement, Fiserv bears a preexisting duty to safeguard FiCare Federal's information in accordance with governing contractual and regulatory standards. Fiserv may not condition its performance of that duty on FiCare Federal's agreement to new or different contractual terms or on the payment of additional fees. FiCare Federal further seeks a declaration that Fiserv's "SecureNow" product does not satisfy Fiserv's existing contractual and regulatory obligations to appropriately protect FiCare Federal's information.

137. **Unenforceability of Master Agreement's Exculpatory and Limitation-of-Liability Provisions (Public Policy).** FiCare Federal is entitled to a declaration that the exculpatory and limitation-of-liability provisions in the Master Agreement are unenforceable because they purport to allow Fiserv to exempt itself from liability for damages caused by its grossly negligent, intentional, fraudulent, tortious, or other conduct for which an exculpatory provision or a limitation-of-liability provision is against public policy.

138. **Fiserv's Defective Purported Automatic Renewal of the Master Agreement (N.Y. General Obligations Law § 5-903).** FiCare Federal is entitled to a declaration that, pursuant to N.Y. General Obligations Law § 5-903, the Master Agreement is unenforceable by Fiserv because it failed to give the statutorily required notice to FiCare Federal before purporting to effectuate an automatic renewal of the Master Agreement.

139. **No Obligation to Pay Early Termination Fees, Liquidated Damages, Deconversion, or Post-Termination Fees (Contract Defenses and Public Policy).** FiCare Federal is entitled to declarations that it has no obligation to pay Fiserv early termination fees, liquidated damages, "deconversion," or other post-termination fees because of the following:

a. Fiserv has no right to enforce the Master Agreement due to its material breaches, repudiation, fraudulent inducement,

fraudulent performance, failure of consideration, commercial impracticability, frustration of purpose, and violation of N.Y. General Obligations Law § 5-903.

b. The fees at issue, other than liquidated damages, are not quantified in the Master Agreement and therefore unenforceable under the doctrine of indefiniteness and because they are not reasonable.

c. The early termination fees or liquidated damages provisions are unenforceable in a renewal term of the Master Agreement. The Master Agreement contemplated an initial term, during which FiCare Federal paid and Fiserv received the complete economic benefit of the parties' bargain, including recurring fee revenue. Fiserv's attempt to impose early termination fees or liquidated damages during a renewal term is improper because the purpose of the liquidated damages clause (if valid during the initial term) would be to compensate Fiserv for unrecovered upfront investments. In the renewal term, those investments have already been recouped in full or substantially recouped, and the clause serves no compensatory function. The liquidated damages provision is not calibrated to reflect any actual damages arising

from an early termination during a renewal term. The same amount is demanded regardless of whether the Master Agreement is terminated in an initial term or renewal term. The formula—80% of all fees remaining in an initial or renewal term—creates a perverse and unreasonable result. Had the parties chosen not to renew at the conclusion of the initial term, no liquidated damages would have applied. Yet if the relationship ended just one day after, Fiserv would claim entitlement to liquidated damages in the millions. This arbitrariness renders the clause punitive in nature, unrelated to any reasonable forecast of actual damages, and unenforceable as a matter of law. The provision fails to be enforceable because it imposes a penalty rather than approximating actual damages, does not decrease or scale based on the elapsed term, bears no reasonable relationship to Fiserv's actual damages, and seeks to unjustly enrich Fiserv by awarding a windfall for services not rendered and that Fiserv has no intention to perform.

d. The early termination fees or liquidated damages provisions are unenforceable penalties because they purport to entitle Fiserv to payment without regard to Fiserv's own wrongful conduct, and

without regard to the substantial independent reasons why FiCare Federal may seek to terminate the Master Agreement to ensure its members are properly protected. The only legitimate purpose of such provisions would be to compensate for actual harm that is difficult to quantify. But if such provisions coerce action or punish—as they do here—they are unenforceable penalties. The plain purpose of these provisions is to coerce FiCare Federal into maintaining its relationship with Fiserv. Moreover, even if these provisions are not unenforceable penalties, to the extent Fiserv relies on them for indemnification or recovery of amounts incurred as a result of its own wrongful acts, such provisions are unenforceable under New York law.

WHEREFORE, FiCare Federal respectfully requests that judgment be entered in its favor on Count 4 for declaratory relief, costs of litigation (including attorneys' fees and costs), and such other and further relief to FiCare Federal as the Court deems appropriate under the circumstances.

Fifth Claim for Relief
Unjust Enrichment
(Against Fiserv Solutions Only)

140. FiCare Federal repeats the allegations in the preceding paragraphs.

141. Fiserv Solutions induced FiCare Federal to pay it by issuing invoices. These invoices, delivered on a recurring basis, conveyed expressly and by implication that the invoiced services had been properly performed and that the invoiced amounts were owed to Fiserv Solutions.

142. In reality, Fiserv Solutions had not performed as promised. Fiserv Solutions' invoices overstated the amounts FiCare Federal owed, and Fiserv Solutions refused to substantiate the invoiced amounts with audit records and withheld material facts about the security deficiencies in its systems. Fiserv Solutions' systems were so insecure that they were not even minimally suitable for storing a regulated credit union's confidential information.

143. As a result of this misconduct, FiCare Federal mistakenly conferred a benefit on Fiserv Solutions in the form of payments for deficient or non-performed services.

144. Fiserv Solutions was unjustly enriched by those payments. Equity and good conscience require Fiserv Solutions disgorge and make restitution of the amounts FiCare Federal paid, with interest.

WHEREFORE, FiCare Federal respectfully requests that judgment be entered in its favor on Count 5 for monetary damages, restitution and disgorgement, costs of litigation (including attorneys' fees and costs), and such

other and further relief to FiCare Federal as the Court deems appropriate under the circumstances.

Sixth Claim for Relief
Defend Trade Secrets Act
(18 U.S.C. § 1836, *et seq.*)

145. FiCare Federal repeats the allegations in the preceding paragraphs.

146. FiCare Federal is the owner of all right, title, and interest in and to certain valuable trade secrets relating to its business operations. FiCare Federal's trade secrets include, but are not limited to, the identities and contact information of its members and employees, the compilation of members' financial history and transactions as reflected on account records and information, and credit information.

147. FiCare Federal's trade secrets are related to products and services used in and intended to be used in interstate and foreign commerce.

148. Other than through unlawful acquisition, the trade secrets are not known to the public and are not readily ascertainable by proper means to persons who could derive value from their disclosure or use.

149. FiCare Federal has taken reasonable measures to maintain the secrecy of its trade secrets, including insisting that Fiserv protect their secrecy pursuant to the Master Agreement and Fiserv's Privacy Notice.

150. FiCare Federal has invested substantial resources in developing and protecting its trade secrets. FiCare Federal's trade secrets provide it with economic advantages over its competitors.

151. Fiserv knew or should have known that FiCare Federal's information at issue comprised FiCare Federal's trade secrets.

152. Fiserv misappropriated and continued to misappropriate FiCare Federal's trade secrets by acquiring and continuing to acquire them through improper means, including by misrepresenting to FiCare Federal the existence and nature of Fiserv's security controls. Had Fiserv provided truthful information to FiCare Federal, it would not have furnished its trade secrets to Fiserv and allowed, and continued to allow, those trade secrets to be stored and accessible on Fiserv's insecure systems.

153. Fiserv also misappropriated FiCare Federal's trade secrets by disclosing them to hackers.

154. At the time of Fiserv's use and disclosure of FiCare Federal's trade secrets, Fiserv knew or had reason to know that it acquired the trade secrets by improper means, under circumstances giving rise to a duty to maintain their secrecy or limit their use, from or through a person who had a duty to FiCare Federal to maintain the trade secrets' secrecy and limit their use, or by mistake prior to a material change of Fiserv's position.

155. Fiserv's misappropriation of FiCare Federal's trade secrets was done for its own commercial advantage, allowing Fiserv to obtain and retain excessive payments from FiCare Federal.

156. Fiserv's acts constitute violations of the Defend Trade Secrets Act, 18 U.S.C. § 1836, *et seq.*

157. Fiserv's misappropriation was willful and malicious, entitling FiCare Federal to exemplary damages under 18 U.S.C. § 1836(b)(3)(C) and reasonable attorneys' fees under 18 U.S.C. § 1836(b)(3)(D).

158. As a direct and proximate result of Fiserv's misappropriation of FiCare Federal's trade secrets, FiCare Federal has suffered and will continue to suffer damages and harm.

WHEREFORE, FiCare Federal respectfully requests that judgment be entered in its favor on Count 6 for monetary damages, injunctive relief, costs of litigation (including attorneys' fees and costs), and such other and further relief to FiCare Federal as the Court deems appropriate under the circumstances.

Seventh Claim for Relief
Fraud / Fraudulent Inducement

159. FiCare Federal repeats the allegations in the preceding paragraphs.

160. Fiserv fraudulently misrepresented its data security practices and knowingly concealed their profound deficiencies, as well as Fiserv's intention to perform under the Master Agreement.

161. Relying on these deceptive assurances, FiCare Federal contracted and continued to remain in a contractual relationship with Fiserv Solutions and entrusted Fiserv with sensitive information, a trust Fiserv intentionally violated.

162. As set forth above, Fiserv fraudulently misrepresented the existence and nature of the security controls that were in place to protect FiCare Federal's confidential information.

163. As set forth above, Fiserv also fraudulently represented its performance and intention to perform under the Master Agreement, including by withdrawing security features mid-contract and forcing upgrades to "SecureNow."

164. Fiserv also fraudulently represented its "Enhanced Authentication" service to FiCare Federal. As set forth above, "Enhanced Authentication" fails to provide MFA that meets baseline standards for authentication. It is therefore not sufficient authentication at all. And it is certainly not "advanced."

165. Further, independent of any specific misrepresentations made by Fiserv, FiCare Federal reasonably and justifiably relied on Fiserv to provide a service with at least minimally adequate measures to protect the confidentiality of FiCare Federal's information and FiCare Federal is entitled to presume, and did expect, that Fiserv would take appropriate measures to keep its information safe.

166. Fiserv did not disclose at any time to FiCare Federal that its information was vulnerable to hackers because Fiserv's security was inadequate. Fiserv was the only one in possession of that material information, which it had a duty to disclose. Fiserv misrepresented, both by affirmative conduct and by omission, the security of its systems, their ability to authenticate authorized users, and their ability to safely store and process FiCare Federal's information, and the security measures and services that have been provided to FiCare Federal.

167. Fiserv also engaged in deception by actively concealing (a) Fiserv's failure to implement reasonable and appropriate security measures, (b) Fiserv's failure to follow industry standards and regulatory guidelines for data security; (c) information about Fiserv's security problems (including by threatening another Fiserv customer who uncovered a security problem with litigation); (d) Fiserv's failure to comply with its own policies, notices, and agreements.

168. FiCare Federal justifiably relied on Fiserv, which had a duty to disclose material facts that would undermine FiCare Federal's reasonable reliance on these subjects. Fiserv has special knowledge of information regarding these subjects that is not reasonably ascertainable by FiCare Federal.

169. FiCare Federal reasonably and justifiably relied on Fiserv's misrepresentations, concealments, acts, and omissions to its detriment by, among

other things, entering into the Master Agreement and other transactions with Fiserv, making payments to Fiserv, continuing to remain in a contractual relationship with Fiserv, and furnishing confidential information to Fiserv.

170. Fiserv knew or should have known that its misrepresentations, concealments, acts, and omissions were false or recklessly made without regard to their falsity, were material to FiCare Federal, and were made with the intent of misleading FiCare Federal into relying upon them, and FiCare Federal did so justifiably rely.

171. Further, the falsity of Fiserv's misrepresentations, concealments, acts, and omissions was within Fiserv's peculiar knowledge and could not have been reasonably discovered by FiCare Federal.

172. By Fiserv's misrepresentations, concealments, acts, and omissions, Fiserv defrauded FiCare Federal, including fraudulently inducing FiCare Federal to contract with, and continue to receive services from, Fiserv. As a direct and proximate result of Fiserv's fraud, FiCare Federal has suffered and will continue to suffer damages and harm.

WHEREFORE, FiCare Federal respectfully requests that judgment be entered in its favor on Count 7 for monetary damages, rescission, restitution and disgorgement, indemnification, declaratory relief, specific performance, injunctive relief, costs of litigation (including attorneys' fees and costs), and such

other and further relief to FiCare Federal as the Court deems appropriate under the circumstances.

Eighth Claim for Relief
Florida Deceptive and Unfair Trade Practices Act
(Fla. Stat. § 501.201 *et seq.*)

173. FiCare Federal repeats the allegations in the preceding paragraphs.

174. A defendant is liable under the Florida Deceptive and Unfair Trade Practices Act (Fla. Stat. 501.201 *et seq.*) if it (1) engages in a deceptive act or unfair practice in the conduct of any trade or commerce (2) which proximately caused an actual injury to the plaintiff or to its business.

175. As set forth above, through its acts, omissions, misrepresentations, and concealments, Fiserv engaged in deceptive and unfair trade acts and practices.

176. Without limitation, Fiserv deceptively and unfairly misrepresented the existence and nature of the security controls that were in place to protect FiCare Federal's confidential information, including by providing false and materially misleading statements to FiCare Federal and Fiserv's other financial institution customers in Fiserv's Compliance Package, Privacy Notice, and other communications.

177. As set forth above, Fiserv also deceptively and unfairly represented its service offerings as well as its performance and intention to perform under the Master Agreement.

178. As set forth above, Fiserv acted deceptively and unfairly by withdrawing security features mid-contract and forcing FiCare Federal and Fiserv's other financial institution customers to upgrade to "SecureNow." Fiserv deceptively and unfairly markets SecureNow because it fails to provide security appropriate for regulated financial institutions, and, contrary to Fiserv's statements, FiCare Federal and Fiserv's other financial institution customers do not need to purchase additional upgrades to obtain Fiserv's preexisting contractual duty to have information safeguarded.

179. Fiserv also unfairly and deceptively represented its "Enhanced Authentication" service to FiCare Federal and Fiserv's other financial institution customers. As set forth above, "Enhanced Authentication" fails to provide MFA that meets baseline standards for authentication. It is therefore not sufficient authentication at all. And it is certainly not "advanced." These representations are deceptive and unfair.

180. Further, independent of any specific misrepresentations made by Fiserv, FiCare Federal reasonably and justifiably relied on Fiserv to provide a service with at least minimally adequate measures to protect the confidentiality

of FiCare Federal's information and FiCare Federal is entitled to presume, and did expect, that Fiserv would take appropriate measures to keep its information safe.

181. Fiserv did not disclose at any time to FiCare Federal that its information was vulnerable to hackers because Fiserv's security was inadequate. Fiserv was the only one in possession of that material information, which it had a duty to disclose. Fiserv engaged in deceptive acts and unfair practices, both by affirmative conduct and by omission, by deceptively and unfairly representing the security of its systems, their ability to authenticate authorized users, and their ability to safely store and process FiCare Federal's information, and the security measures and services that have been provided to FiCare Federal.

182. Fiserv also engaged in deception and unfair practices by actively concealing (a) Fiserv's failure to implement reasonable and appropriate security measures, (b) Fiserv's failure to follow industry standards and regulatory guidelines for data security; (c) information about Fiserv's security problems (including by threatening another Fiserv customer who uncovered a security problem with litigation); (d) Fiserv's failure to comply with its own policies, notices, and agreements.

183. Fiserv's actions affected commerce because they were done in pursuit of business from FiCare Federal.

184. Fiserv's deceptive acts and unfair practices have harmed FiCare Federal and other financial institutions that are Fiserv customers.

185. Fiserv proximately caused FiCare Federal actual injury. Had Fiserv provided FiCare Federal with truthful information and not engaged in deceptive and unfair practices, FiCare Federal would not have entered into the Master Agreement and other transactions with Fiserv, made payments to Fiserv, furnished confidential information or trade secrets to Fiserv, or allowed trade secrets or confidential information to be stored and accessible on Fiserv's insecure systems.

186. FiCare Federal is entitled to attorneys' fees under Fla. Stat. § 501.211(2).

187. As a direct and proximate result of Fiserv's deceptive and unfair practices, FiCare Federal has suffered and will continue to suffer damages and harm.

WHEREFORE, FiCare Federal respectfully requests that judgment be entered in its favor on Count 8 for monetary damages, rescission, restitution and disgorgement, indemnification, declaratory relief, specific performance, injunctive relief, costs of litigation (including attorneys' fees and costs), and such other and further relief to FiCare Federal as the Court deems appropriate under the circumstances.

Jury Trial Demand

FiCare Federal requests a trial by jury of all issues so triable.

Demand for Relief

WHEREFORE, FiCare Federal respectfully requests that the Court enter final judgment on the Complaint in favor of FiCare Federal and against Defendants and grant the following relief:

(i) **Monetary damages**, including, without limitation, restitutionary, compensatory, consequential, incidental, reliance, statutory, and punitive—all in amounts to be determined at trial;

(ii) **Rescission of the Master Agreement**, unwinding the parties' relationship;

(iii) **Restitution and disgorgement**, restoring FiCare Federal to the status quo ante, including, without limitation, recovery of amounts FiCare Federal paid to Fiserv under the Master Agreement for services that were materially deficient, nonconforming, or rendered valueless by Fiserv's breaches and repudiation;

(iv) **Indemnification** of FiCare Federal's losses;

(v) **Declaratory relief** declaring the parties' respective rights and obligations in connection with the Master Agreement;

(vi) **Specific performance** compelling Fiserv to perform its obligations to FiCare Federal;

(vii) **Preliminary and permanent injunctive relief** protecting FiCare Federal against additional harm;

(viii) **Costs of litigation**, including, without limitation, FiCare Federal's attorneys' fees and costs, and the maximum prejudgment and postjudgment interest allowed by law; and

(ix) **Any further relief** that may be necessary to achieve justice.

Dated: January 27, 2026

Respectfully submitted,

Charles J. Nerko (Lead Counsel)*
John C. Cleary*
Walter E. Swearingen*
NERKO PLLC
1178 Broadway, 3rd Floor
New York, New York 10001
518.363.9100
cnerko@nerko.com
jcleary@nerko.com
wswearingen@nerko.com

and

/s/ John N. Muratides
John N. Muratides (Florida Bar No. 332615)
Primary: jmuratides@stearnsweaver.com
Secondary: mbumoskey@stearnsweaver.com
Darrin J. Quam (Florida Bar No. 995551)
Primary: dquam@stearnsweaver.com
Secondary: mbumoskey@stearnsweaver.com
STEARNS WEAVER MILLER WEISSLER ALHADEFF & SITTERSON, P.A.
Post Office Box 3299
401 E. Jackson St., Suite 2100
Tampa, Florida 33601
Telephone: 813.223.4800
Facsimile: 813.222.5089

Attorneys for Plaintiff
FiCare Federal Credit Union

* Not admitted in this Court; *pro hac vice* application to be filed