UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF FLORIDA
FORT LAUDERDALE DIVISION

AMANDA FISCHER, individually and on behalf of all similarly situated persons, Plaintiff, v. CENTRALSQUARE TECHNOLOGIES, LLC Defendants.	CASE NO. 0:21-CV-60856 CLASS ACTION COMPLAINT JURY TRIAL DEMANDED

Plaintiff Amanda Fischer, on behalf of herself and all similarly situated persons, brings this Petition against Defendant CentralSquare Technologies, LLC ("CentralSquare"), based on personal knowledge and the investigation of counsel, and alleges the following:

INTRODUCTION

1. This is an action to recover damages from CentralSquare for the harm it caused Plaintiff and a nationwide class of persons whose payment card information was stolen as a result of a data breach on CentralSquare's payment software, Click2Gov.

2. On October 13, 2017, Superion (now known as CentralSqaure) CEO, Simon Angove, released a statement acknowledging that its Click2Gov online utilities payment portal customers had experienced a data breach.

3. Click2Gov is a payment processing service provided by CentralSquare (formerly known as Superion) and used by municipalities across the United States to collect various payments, including utility bills, parking tickets, taxes, and similar payments.

4. This is far from the first time CentralSquare has suffered a payment card data breach. Since mid-2017, hackers have been attracted to CentralSquare's Click2Gov payment portal

like flies to a carcass. This first wave of cyber hacks against CentralSquare, defined herein as the "Data Breach," began in 2017 and ended in 2018, resulting in cyber criminals stealing the payment card and related information, including names, card numbers, expiration dates, and security codes (collectively, the "Payment Data") of at least 300,000 individuals and selling it to identity thieves on the dark web.[1] The victims were residents of dozens of small-to-medium-sized municipalities across the United States.

5. Many of these Data Breach victims, including Plaintiff and Class Members, suffered fraudulent charges, had their payment cards canceled, lost use of their funds, lost time contesting charges and frantically trying to claw back funds stolen from their bank accounts, driving to and from banks and credit unions, and some have even canceled accounts.

6. That's where the story should have ended: in late 2018, with CentralSquare and its municipal clients so fully on guard against cyber-hackers that nothing like this could happen again. But they weren't, and it did happen again.

7. Beginning in August and ending in October 2019, a second wave of Click2Gov data breaches took place, followed by a third wave of data breaches from April to July 2020.[2]

8. Plaintiff brings this action individually and on behalf of Class Members to hold CentralSquare accountable for the harm it has caused and continues to cause to individuals across the country.

[1]Stas Alforov & Christopher Thomas, *Second Wave of Click2Gov Breaches Hits United States*, GEMINI ADVISORY (Sept. 19, 2019), https://geminiadvisory.io/second-wave-of-click2gov-breaches-hits-united-states/.
[2] *See* https://statescoop.com/click2gov-breaches-eight-cities-magecart/.

PARTIES

9. Plaintiff Amanda Fischer is and at all relevant times to this action was a citizen of Florida and a resident of the City of Margate, Broward County, Florida.

10. Defendant CentralSquare Technologies, LLC, is a Delaware limited liability company headquartered at 1000 Business Center Dr., Lake Mary, Florida 32746. Upon information and belief, CentralSquare is a citizen of Florida.

11. CentralSquare is a company whose mission is "[t]o create the broadest, smartest and most agile software platform for building safer, smarter communities."[3]

12. CentralSquare also represents itself as the go-to payment technology provider for public entities:

> A central square is a place where citizens interact with their government, whether it be at city hall, police or fire station, or a hospital. "To square" is designed to communicate taking communities to the next level, and the four corners of a square refer to the four businesses that came together to form CentralSquare. CentralSquare emphasizes putting citizens at the center of everything we offer. We partner with more than 7,500 public sector agencies across North America, bringing together two primary drivers for improving people's lives—technology and government"[4]

JURISDICTION AND VENUE

13. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are more than 100 putative class members, and at least some members of the proposed Class have a different citizenship from CentralSquare.

14. This Court has jurisdiction over CentralSquare as it is incorporated and has its principal place of business in Florida.

[3] "About Us," CentralSquare Technologies, https://www.centralsquare.com/about-us, (last visit on April 14, 2020).
[4] *Id*.

15. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District and CentralSquare has caused harm to Class Members residing in this District.

STATEMENT OF FACTS

A. The Data Breaches

16. As early as the spring of 2017, numerous reports from local news outlets began to report on instances of payment card data breaches that were linked to local utility payment systems. As researchers and reporters honed in, all fingers began to point to one source: CentralSquare's Click2Gov software.[5]

17. In October 2017, CEO Simon Angove of CentralSquare (known at that time as Superion) publicly acknowledged the growing number of data security incidents. He stated:

> Recently we received reports of suspicious activity involving a small number of our customers' computer networks, including possible attempts to steal personally identifiable information. . . . We have notified Superion customers about the suspicious activity and have continued to work closely with the small number of affected customers throughout our investigation. As part of our investigation we have identified and notified our customers of certain potential vulnerabilities in the security of their network and provided them with recommendations for addressing the same.[6]

18. CentralSquare's "recommendations" notwithstanding, this "small number of affected customers" proved to be but the nose of the camel.

19. The Data Breach, which encompassed 2017 through 2018, started with locally hosted Click2Gov software systems at individual municipalities, as opposed to cloud-based Click2Gov software hosted directly by CentralSquare.

---

[5]Stas Alforov, *Dozens of Municipalities Exposed in Click2Gov Software Compromise*, GEMINI ADVISORY (Dec. 18, 2018), https://geminiadvisory.io/hacked-click2gov-exposed-payment-data/.

[6]*CEO Response to Reported Breach*, CENTRALSQUARE, FORMERLY SUPERION (Oct. 13, 2017), available at https://web.archive.org/web/20181202233703/www.superion.com/ceo-response-to-reported-breach/.

20. As a result, the Payment Data of tens of thousands of individuals who made payments through the Click2Gov portal at dozens of cities, including Margate, was stolen and sold on black markets on the dark web because of CentralSquare's negligence in its failure to regularly and adequately monitor its systems and address the various vulnerabilities in its Click2Gov software by providing adequate patches to the municipalities.

a. The 2017/2018 Data Breach

21. In December 2018, Gemini Advisory covered a breach of CentralSquare's Click2Gov payment portal that affected dozens of cities across the United States and Canada between 2017 and late 2018.[7] A depiction of the impacted cities from the Data Breach and subsequent data breaches are shown here[8]:

Image 1: Map depicting cities affected only by the original Click2Gov breach (yellow and those affected by the second wave of Click2Gov breaches (blue).

[7] *See* https://geminiadvisory.io/second-wave-of-click2gov-breaches-hits-united-states/.
[8] *Id*.

22. During the Data Breach, over 300,000 "Card Not Present" records were compromised across a variety of U.S. cities using Click2Gov.[9]

23. In June 2018, CentralSquare released a statement in which it claimed to have addressed the issue with the Click2Gov payment portal system by deploying necessary patches to the impacted municipalities, including Margate, thus making it clear that the Data Breach was preventable and could have been prevented had CentralSquare timely deployed the necessary updates to the municipalities' Click2Gov payment systems.

24. Because of CentralSquare's specialization in online secure payment processing for public entities, it was on notice of the ever-present and significant threat of Payment Data theft if it did not adequately maintain vigilant and updated security practices. CentralSquare had or should have had knowledge of the very serious risks associated with payment card data breaches, and of the need to ensure that its own systems were adequately secured. However, it willfully failed to make the necessary updates to its security practices, protocols, and Click2Gov system, thus permitting the Data Breach to occur.

25. CentralSquare, at all times relevant to this action, had duties to Plaintiff and members of the class to: (a) properly secure Payment Data submitted to or collected at municpality locations and on the impacted municipalities' internal networks; (b) encrypt Payment Data using industry standard methods; (c) use available technology to defend its systems from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiff and the Class that naturally result from Payment Data theft; and (e) promptly notify municipality customers and impacted citizens when it became aware of the potential that citizens' Payment Data may have been compromised.

[9] *Id*.

26. As a result of the Data Breach, many of the victims, including Plaintiff and Class Members, have suffered fraudulent charges, had their payment cards canceled, lost use of their funds, lost time contesting charges and frantically trying to claw back funds stolen from their bank accounts, driving to and from banks and credit unions, and some have even had to cancel accounts.

27. CentralSquare's failure to adequately protect Plaintiff and Class Members' Payment Data also caused significant additional harms, including the time-consuming requirement to constantly scrutinize bank statements, obtaining and paying for credit monitoring, checking credit reports, contesting false charges, and other efforts that require extensive amounts of time—and often out-of-pocket expenses—while CentralSquare has done little to nothing to assist the individuals affected by the Data Breach, including failure to provide free credit monitoring services.

28. Defendants have shifted the risk and responsibility for their own negligent failures and breaches onto the innocent utilities customers.

29. As a result of the Data Breach, Plaintiff and Class Members suffered actual fraud and losses, including money being stolen from their bank accounts or from their credit accounts, loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; lost control over the value of personal information; unreimbursed losses relating to fraudulent charges; losses and fees relating to exceeding credit and debit card limits, balances, and bounced transactions; harm resulting from damaged credit scores and information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Payment Data.

B. Industry Standards and Governmental Guidance for Protection of Payment Data

30. Payment card processing companies have issued rules and standards governing the basic measures that merchants and payment software companies, including CentralSquare, must take to ensure that consumers' valuable Payment Data is protected.

31. The Payment Card Industry Data Security Standard ("PCI DSS") is a list of twelve information security requirements that were promulgated by the Payment Card Industry Security Standards Council. The PCI DSS list applies to all organizations and environments where cardholder data is stored, processed, or transmitted, and requires CentralSquare to protect cardholder data, ensure the maintenance of vulnerability management programs, implement strong access control measures, regularly monitor and test networks, and ensure the maintenance of information security policies.

32. The twelve requirements of the PCI DSS are:

a. Install and maintain a firewall configuration to protect cardholder data;

b. Do not use vendor-supplied defaults for system passwords and other security parameters;

c. Protect stored cardholder data;

d. Encrypt transmission of cardholder data across open, public networks;

e. Protect all systems against malware and regularly update anti-virus software or programs;

f. Develop and maintain secure systems and applications;

g. Restrict access to cardholder data by business need to know;

h. Identify and authenticate access to system components;

i. Restrict physical access to cardholder data;

j. Track and monitor all access to network resources and cardholder data;

k. Regularly test security systems and processes; and

l. Maintain a policy that addresses information security for all personnel.[10]

33. Furthermore, PCI DSS sets forth detailed and comprehensive requirements that must be followed to meet each of the twelve mandates.

34. CentralSquare was at all times relevant fully aware of its data protection obligations in light of its participation in the payment card processing networks.

35. Additionally, according to the Federal Trade Commission ("FTC"), the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45. *See, e.g., F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 245-47 (3d Cir. 2015); I*n re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005).

36. As long ago as 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the personal customer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommend that businesses use intrusion detection systems to expose a breach as soon as it occurs; monitor all incoming traffic for suspicious activity; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

[10]Payment Card International (PCI) Data Security Standard, "Requirements and Security Assessment Procedures, Version 3.2.1," (May 2018), https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1574069601944.

37. The FTC has issued orders and received judgments against businesses that failed to employ reasonable measures to secure Payment Card Data. The FTC orders provide further notice and direction to businesses regarding their data security obligations. *See, e.g.*, *Wyndham Worldwide Corp.*, 799 F.3d at 245-47; I*n re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465.

38. CentralSquare failed to meet its obligations under the FTC Act and FTC guidance, and failed to comply with the PCI DSS standards.

39. Upon information and belief, CentralSquare had actual knowledge of the vulnerability of its Click2Gov software and that hackers were actively trying to exploit it and, despite this knowledge, willfully failed to make the necessary changes to its security practices and protocols.

40. CentralSquare's reckless security practices in the face of a known threat permitted hackers to steal the Payment Data of tens of thousands of individuals.

C. Plaintiff Fischer's Experiences

41. Plaintiff Fischer used her debit card to pay her City of Margate utility bill online through CentralSquare's Click2Gov program.

42. On three separate occasions, Plaintiff discovered that someone had stolen money from her checking account. Between April 2017 and August 2017, three fraudulent transactions were made using the debit card that she used to pay her Margate water bill on the Click2Gov software. Altogether, a thief stole over $366.74 from her bank checking account.

43. Each time she discovered the stolen funds, Plaintiff called her bank and reported the fraudulent transactions.

44. Plaintiff contested these transactions with her bank, which canceled her debit card

each time she called in to report a new fraudulent transaction, leaving her without access to her checking account for days at a time. The bank eventually "provisionally" credited the stolen money back to her account while it investigated, but it warned her that it could claw back the money depending on the investigation, leaving her not knowing whether the money would be clawed back or not, which limited her use of her money.

45. It was in August 2017 that she became aware of the Data Breach through a City of Margate social media post, which informed the citizens of Margate of the Data Breach (and compromise of citizens' Payment Data resulting therefrom). A screenshot of the social media post is attached hereto as **Exhibit 1**.

46. Fischer subsequently filed a police report with the City of Margate Police Department, notifying them of the fraudulent transactions that had occurred using the same debit card that she used to pay her Margate water bill.

47. Fischer spent over six hours of her time responding to the Data Breach, including contesting the fraudulent charges, requesting new debit cards, filing a police report, and reviewing statements.

D. Plaintiff and Class Members Suffered Damages

48. As alleged throughout this Complaint, Plaintiff and Class Members have suffered injuries in fact that are fairly traceable to the misconduct by Defendant, alleged herein, and such injuries are likely to be redressed by a favorable judicial decision.

49. The Payment Data of Plaintiff and Class Members is private and sensitive in nature and was left inadequately protected by CentralSquare. CentralSquare did not obtain Plaintiff's and Class Members' consent to disclose their Payment Data to any other person, as required by applicable law and industry standards.

50. The Data Breach was a direct and proximate result of CentralSquare's failure to properly safeguard and protect Plaintiff's and Class Members' Payment Data from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including CentralSquare's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class Members' Payment Data to protect against reasonably foreseeable threats to the security or integrity of such information.

51. CentralSquare had the resources to prevent the Data Breach. CentralSquare made significant expenditures to market, promote, and sell its product, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

52. Had CentralSquare remedied the known deficiencies in its Click2Gov payment portal system, followed PCI DSS guidelines, and adopted security measures recommended by experts in the field, CentralSquare would have prevented intrusion into its systems and, ultimately, the theft of Plaintiff's and Class Members' confidential Payment Data.

53. As a direct and proximate result of CentralSquare's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class Members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, inter alia, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. This time has been lost forever and cannot be recaptured.

54. CentralSquare's wrongful actions and inaction directly and proximately caused the theft and dissemination into the public domain of Plaintiff's and Class Members' Payment Data, causing them to suffer, and continue to suffer, economic damages and other actual harm for which they are entitled to compensation, including:

a. theft of their personal and financial information;

b. unauthorized charges on their debit and credit card accounts;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their credit/debit card and personal information being placed in the hands of criminals and misused via the sale of Plaintiff's and Class Members' information on the Internet's black market;

d. the lack of any notification of the Data Breach to Plaintiff and Class Members;

e. the improper disclosure of Plaintiff's and Class Members' Payment Data;

f. loss of privacy;

g. ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the Data Breach;

h. ascertainable losses in the form of deprivation of the value of their PII and Payment Data, for which there is a well-established national and international market;

i. ascertainable losses in the form of the loss of cash back or other benefits as a result of their inability to use certain accounts and cards affected by the Data Breach;

j. loss of use of, and access to, their account funds and costs associated with the inability to obtain money from their accounts or being limited in the amount of

money they were permitted to obtain from their accounts, including missed payments on bills and loans, late charges and fees, and adverse effects on their credit including adverse credit notations; and

k. the loss of productivity and value of their time spent to address, attempt to ameliorate, mitigate, and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, cancelling and reissuing cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and the inconvenience, nuisance and annoyance of dealing with all such issues resulting from the Data Breach.

55. While the Payment Data of Plaintiff and Class Members has been stolen, CentralSquare continues to hold citizen Payment Data, including that of Plaintiff and Class Members. Particularly because CentralSquare has demonstrated a consistent inability to prevent a data breach, Plaintiff and Class Members have an undeniable interest in ensuring that their Payment Data is secure, remains secure, is properly and promptly destroyed, and is not subject to further theft.

CLASS ALLEGATIONS

56. Plaintiff incorporates by reference paragraphs 1-8, 9-12, and 16-55 as if fully set forth herein.

57. Plaintiff, pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3), and (c)(4), brings all claims as class claims and seeks relief on behalf of herself and as a representative of all others who are similarly situated, asserting claims on behalf of the following classes (collectively the "Class Members" or the "Class"):

Nationwide Class against CentralSquare (the "Nationwide Class"):

> All persons whose payment card information was compromised in the 2017/2018 wave of data breaches affecting CentralSquare Technologies, LLC's Click2Gov payment platform.

City of Margate, Florida subclass (the "Margate Subclass"):

> All Margate citizens whose payment card information was compromised in the 2017/2018 wave of data breaches affecting CentralSquare Technologies, LLC's Click2Gov payment platform.

58. Excluded from the Class are Defendant CentralSquare and any entity in which CentralSquare has a controlling interest, as well as CentralSquare's officers, directors, legal representatives, successors, subsidiaries, and assigns. The Class also excludes any judge, justice, or judicial officer presiding over this matter and the members of their immediate families and judicial staff.

59. Plaintiff reserves the right to amend the above class definitions or to seek additional subclasses as necessary.

A. Class Certification is Appropriate

60. The proposed Nationwide Class and Margate Subclass meet the requirements of Rule 23(a), (b)(2), (b)(3), and (c)(4) as required.

61. *Numerosity*: The proposed classes are so numerous that joinder of all members is impracticable. While the total number of individuals affected by the Data Breach is unknown, based on reporting, the Margate Subclass may include several thousand city utilities customers. The Nationwide Class is much larger, including tens of thousands of residents of what appears to be "46 confirmed impacted local governments."[11] *See* Fed. R. Civ. P. 23(a)(1).

[11] *See* https://threatpost.com/patched-click2gov-flaw-still-afflicting-local-govs/140109/.

62. *Commonality and Predominance*: Common questions of law and fact exist to Plaintiff and all members of the proposed Classes. These questions predominate over the questions affecting individual Class Members. These common legal and factual questions include, but are not limited to, the following:

As to the Nationwide Class and CentralSquare:

a. Whether CentralSquare engaged in the wrongful conduct alleged herein;

b. Whether CentralSquare owed a duty to Plaintiff and Class Members to adequately protect their Payment Data, and whether it breached this duty;

c. Whether CentralSquare breached federal and state laws, thereby breaching its duties to Plaintiff and the Classes as a result of the Data Breach;

d. Whether Defendant's contract with the impacted municipalities (and the representations therein) created third-party beneficiary contracts;

e. Whether Defendant breached third-party beneficiary contracts by failing to protect Plaintiff's and Class Members' Payment Data;

f. Whether CentralSquare knew or should have known that its computer and network systems were vulnerable to attacks from hackers and cyber criminals;

g. Whether CentralSquare's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its computer and network systems resulting in the theft of customers' Payment Data;

h. Whether CentralSquare wrongfully failed to inform Plaintiff and Class Members that it did not maintain computer software and other security procedures and precautions sufficient to reasonably safeguard users' sensitive financial and personal data;

i. Whether Plaintiff and members of the Classes suffered injury as a proximate result of CentralSquare's conduct or failure to act;

j. Whether CentralSquare recklessly and willfully violated its duties to Plaintiff and the Nationwide Class; and

k. Whether Plaintiff and the classes are entitled to recover compensatory and punitive damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiff and the Classes;

As to the Margate Subclass and CentralSquare:

a. Whether Defendant's contract with the City of Margate (and the representations therein) created third-party beneficiary contracts;

b. Whether Defendant breached third-party beneficiary contracts by failing to protect Plaintiff's and Subclass Members' Payment Data;

c. Whether Defendant failed to use industry best practices and to comply with FTC guidance to protect Plaintiff and Subclass Members' Payment Data;

d. Whether Defendant sufficiently addressed, remedied, or protected Plaintiff and Subclass Members following the Data Breach and took adequate preventative and precautionary measures to ensure Plaintiff and the Subclass Members would not experience further harm;

e. Whether Defendant received money from Plaintiff and members of the Margate Subclass to provide for secure transactions;

f. Whether Plaintiff and members of the Margate Subclass failed to receive the security they paid for;

g. Whether Plaintiff and members of the Margate Subclass are entitled to reimbursement for money Defendant received from them; and

h. Whether Plaintiff and Subclass Members are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiff and the Classes.

63. These questions are common to all Class Members' claims and predominate over any and all individual claims that might exist. *See* Fed. R. Civ. P. 23(a)(2) and (b)(3).

64. *Typicality*: Plaintiff's claims are typical of the claims of the classes. Plaintiff and all members of the Class were injured through CentralSquare's uniform misconduct. The same event and conduct that gave rise to Plaintiff's claims are identical to those that give rise to the claims of every other member of the Class because Plaintiff and Class Members had their sensitive Payment Data compromised in the same way by the same conduct committed by CentralSquare. *See* Fed. R. Civ. P. 23(a)(3).

65. *Adequacy*: Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class that she seeks to represent; Plaintiff has retained counsel competent and highly experienced in complex litigation (and particularly data breach class action litigation); Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and her counsel. *See* Fed. R. Civ. P. 23(a)(4).

66. *Superiority*: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be difficult, if not impossible, for members of the Class

to individually and effectively redress Defendants' wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court. *See* Fed. R. Civ. P. 23(b)(3).

67. *Injunctive and Declaratory Relief*: Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through its uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

68. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether CentralSquare failed to timely notify of the Data Breach;

b. Whether CentralSquare owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, and safeguarding their Payment Data;

c. Whether CentralSquare's security measures to protect its Click2Gov payment portal system were reasonable in light of the PCI DSS requirements, FTC data security recommendations, and other best practices recommended by data security experts;

d. Whether CentralSquare's failure to adequately comply with PCI DSS standards and/or to institute protective measures beyond PCI DSS standards amounted to negligence;

e. Whether CentralSquare failed to take commercially reasonable steps to safeguard the Payment Data of Plaintiff and Class Members; and

f. Whether adherence to PCI DSS requirements, FTC data security recommendations, and measures recommended by data security experts would have reasonably prevented the Data Breach.

69. Finally, all members of the proposed Class are readily ascertainable. CentralSquare has access to information regarding which of the cities were impacted by the Data Breach. CentralSquare also maintains the information of the impacted citizens on its systems. Using this information, Class Members can be identified, and their contact information ascertained, for the purpose of providing notice to the Class.

CAUSES OF ACTION

COUNT I - NEGLIGENCE
(On behalf of the Nationwide Class or, alternatively, on behalf of the Margate Subclass)

70. Plaintiff realleges and incorporates paragraphs 1-8, 9-12, and 16-69 as though fully set forth herein.

71. CentralSquare collected Payment Data from Plaintiff and Class Members in exchange for public utilities payments and other services available online to Plaintiff.

72. CentralSquare owed a duty to Plaintiff and the Class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their financial and personal information in CentralSquare's possession from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing CentralSquare's networks and

data security systems to ensure that Plaintiff's and Class Members' financial and personal information in CentralSquare's possession was adequately protected in the process of collection and following collection while stored on CentralSquare's systems.

73. CentralSquare owed a duty to Plaintiff and Class Members to implement processes that would detect a breach of its security system in a timely manner and to timely act upon warnings and alerts, including those generated by its customers and own security systems.

74. CentralSquare owed a duty to Plaintiff and Class Members to provide security consistent with industry standards and requirements and to ensure that its computer systems and networks—and the personnel responsible for them—adequately protected the financial and personal information of Plaintiff and Class Members whose confidential data CentralSquare obtained and maintained.

75. CentralSquare knew the risks inherent in collecting and storing the financial and personal information of Plaintiff and Class Members and of the critical importance of providing adequate security for that information.

76. CentralSquare's conduct created a foreseeable risk of harm to Plaintiff and Class Members. This conduct included but was not limited to CentralSquare's failure to take the steps and opportunities to prevent and/or detect and mitigate the impact of the Data Breach. CentralSquare's conduct also included its willful decision not to comply with industry standards for the safekeeping and maintenance of the financial and personal information of Plaintiff and Class Members.

77. As a direct and proximate result of CentralSquare's negligent conduct, Plaintiff and Class Members have been injured and are entitled to actual damages and punitive damages in amounts to be proven at trial.

COUNT II – NEGLIGENCE PER SE
(On behalf of the Nationwide Class or, alternatively, on behalf of the Margate Subclass)

78. Plaintiff realleges and incorporates paragraphs 1-8, 9-12, and 16-69 as though fully set forth herein.

79. Under the FTC Act, 15 U.S.C. § 45 and its implementing regulations and guidance, CentralSquare had a duty to provide fair and adequate payment systems and conform to certain minimum data security practices to safeguard Plaintiff's and Class members' Payment Data.

80. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses like CentralSquare of failing to use reasonable measures to protect Payment Data.

81. CentralSquare violated Section 5 of the FTC Act by failing to use reasonable measures to protect Payment Data and not complying with applicable industry standards, including PCI DSS, as described above and incorporated here. CentralSquare's conduct was particularly unfair and unreasonable given the nature and amount of Payment Data it processed and the foreseeable consequences of a data breach, including the immense damages that would result to consumers.

82. The harm that has occurred is the type of harm the FTC Act is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against business that, through their failure to employ reasonable data security measures, caused the same harm as that suffered by Plaintiff and the Class.

83. CentralSquare's failure to comply with the FTC Act by implementing and maintaining reasonable data security measures constitutes negligence *per se*.

84. But for CentralSquare's breach of its duties owed to Plaintiff and the Class, they would not have been injured.

85. The injuries suffered by Plaintiff and the Class were the reasonably foreseeable (and foreseen) result of CentralSquare's breach of its duties. CentralSquare knew that it was failing to meet its duties and that its breach would cause Plaintiff and the Class to suffer the foreseeable harms.

86. Accordingly, Plaintiffs and Class Members are entitled to actual and punitive damages in an amount to be proven at trial, along with the costs and attorney fees incurred in this action.

COUNT III – BREACH OF THIRD-PARTY BENEFICIARY CONTRACT
(On behalf of the Nationwide Class or, alternatively, on behalf of the Margate Subclass)

87. Plaintiff realleges and incorporates paragraphs 1-8, 9-12, and 16-69 as though fully set forth herein.

88. CentralSquare entered into a contract with Margate and all other impacted municipalities to provide secure payment card processing services for the cities' utilities customers. CentralSquare entered into substantially identical contracts with each of the cities affected in the Data Breach.

89. These contracts were made expressly for the benefit of Plaintiff and the Class, as it was their Payment Data that CentralSquare agreed to protect.

90. CentralSquare knew that if it were to breach these contracts with the cities, the citizen consumers would be harmed, including by fraudulent transactions and related harms.

91. CentralSquare breached its contracts with the cities affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach.

92. As foreseen, Plaintiff and the Class were harmed by CentralSquare's breach, including fraudulent charges and related injuries.

93. Accordingly, Plaintiff and the Class are entitled to damages in an amount to be determined at trial, along with their costs and attorney fees incurred in this action.

COUNT IV – BREACH OF CONFIDENCE
(On behalf of the Nationwide Class or, alternatively, on behalf of the Margate Subclass)

94. Plaintiff realleges and incorporates paragraphs 1-8, 9-12, and 16-69 as though fully set forth herein.

95. At all times during Plaintiff's and Class Members' utilization of Defendant's Click2Gov payment platform, Defendant was fully aware of the confidential and sensitive nature of Plaintiff's and Class Members' Payment Data that they were providing to Defendant.

96. As alleged herein and above, Plaintiff and Class Members had an expectation that their Payment Data would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

97. Plaintiff and Class Members provided their respective Payment Data to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the Payment Data to be disseminated to any unauthorized parties.

98. Plaintiff and Class Members also provided their respective Payment Data to Defendant with the explicit and implicit understanding that Defendant would take precautions to protect their Payment Data from unauthorized disclosure, such as following basic principles of information security practices.

99. Defendant voluntarily received in confidence Plaintiff's and Class Members' Payment Data onto its Click2Gov payment portal system with the understanding that the Payment Data would not be disclosed or disseminated to the public or any unauthorized third parties.

100. Due to Defendant's failure to prevent, detect, and/or avoid the Data Breach from occurring by, *inter alia*, failing to follow best information security practices to secure Plaintiff's

and Class Members' Payment Data, Plaintiffs' and Class Members' Payment Data was disclosed and misappropriated to unauthorized parties, including to unauthorized parties on the dark web, beyond Plaintiffs' and Class Members' confidence, and without their express permission.

101. As a direct and proximate result of Defendant's actions and inaction, Plaintiff and Class Members have suffered damages.

102. But for Defendant's unauthorized disclosure of Plaintiff's and Class Members' Payment Data in violation of the parties' understanding of confidence, their Payment Data would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiff's and Class Members' Payment Data, as well as the resulting damages.

103. The injury and harm Plaintiff and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiff's and Class Members' Payment Data. Defendant knew its Click2Gov payment portal system and technology had numerous security vulnerabilities.

104. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and the Class have suffered injuries and damages arising from identity theft; Plaintiff's and Class Members' inability to use their debit or credit cards because those cards were cancelled, suspended, or otherwise rendered unusable as a result of the Data Breach and/or false or fraudulent charges stemming from the Data Breach, including but not limited to late fees charged; damages from lost time and effort to mitigate the actual and potential impact of the Data Breach on their lives, including, *inter alia*, by contacting their financial institutions, closing or modifying their financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports.

105. As a direct and proximate result of Defendant's breaches of confidence, Plaintiff and Class Members have suffered emotional distress, loss of privacy, and other economic and non-economic losses.

PRAYER FOR RELIEF

Plaintiff Fischer, on behalf of herself and all others similarly situated, respectfully requests that the Court grant the following relief:

a. Certifies a nationwide class against Defendant CentralSquare and a subclass of affected residents in the City of Margate, Florida;

b. Award Plaintiff and the Class appropriate monetary relief, including actual damages, punitive damages, restitution, and disgorgement.

c. Award Plaintiff and the Class equitable, injunctive and declaratory relief as may be appropriate; Plaintiff, on behalf of the class, seeks appropriate injunctive relief designed to protect against the recurrence of a data breach by adopting and implementing best security data practices to safeguard customers' financial and personal information, and an extension of credit monitoring services and similar services to protect against all types of identity theft, especially including card theft and fraudulent card charges;

d. Enter an order requiring Defendants to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;

e. Enter judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorney fees, costs and expenses as allowably by law; and

f. Any other favorable relief as allowable under law or at equity.

Dated: April 21, 2021

Respectfully Submitted,

/s/ David J. George
David J. George, Esq. (FL Bar No. 0898570)
Brittany L. Brown, Esq. (FL Bar No. 105071)
GEORGE GESTEN MCDONALD, PLLC
9897 Lake Worth Road, Suite #302
Lake Worth, FL 33467
Phone: (561) 232-6002
Fax: (888) 421-4173
Email: DGeorge@4-Justice.com
E-Service: eService@4-Justice.com

*William B. Federman, OBA # 2853
*Tyler J. Bean, OBA # 33834
FEDERMAN & SHERWOOD
10205 N. Pennsylvania
Oklahoma City, OK 73120
Telephone: (405) 235-1560
Facsimile: (405) 239-2112
wbf@federmanlaw.com
tjb@federmanlaw.com

Attorneys for Plaintiff and the Putative Class
**To be admitted pro hac vice*