IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

SANGER POWERS and ROBERT LEGG, individually and on behalf of all others similarly situated,	)	**CASE NO. 20-cv-982**
Plaintiffs,	)	**CLASS ACTION COMPLAINT**
v.	)	
FILTERS FAST, LLC,	)	
Defendant.	)	**JURY TRIAL DEMANDED**

Plaintiffs Sanger Powers ("Powers") and Robert Legg ("Legg") (collectively, "Plaintiffs"), individually and on behalf of all similarly situated persons, allege the following against Defendant Filters Fast, LLC ("Filters Fast" or "Defendant") based on personal knowledge as to their own experiences and on information and belief from the investigation of counsel.

INTRODUCTION

1. In this action, Plaintiffs seek to hold Filters Fast responsible for the harm it caused them and thousands of other customers in the massive data breach that took place between July 15, 2019 and July 10, 2020 (the "Data Breach").

2. Due to Defendant's negligence and failure to enforce adequate data security, for nearly a full year, cyber criminals were able to infiltrate Filters Fast's computer systems, install malicious code to the website, and steal the personal information and financial data of millions of unsuspecting customers across the country. Filters Fast's negligent failure to meet industry standards of cyber security allowed this to happen.

3. Because of Filters Fast's inadequate and negligent security measures and failure to adequately monitor its website and checkout system, cyber criminals were able to steal vast

amounts of sensitive personal information, including credit card and debit card numbers, expiration dates, cardholder names, Card Verification Value (CVV) numbers, and other card information (collectively, "Payment Data").

4. Filters Fast first announced the Breach in a Notice of Data Breach sent to customers in August 2020, months after it knew it had suffered a massive data breach.

5. Although Filters Fast was aware of the Data Breach as early as February 2020, it did not take its website offline while it investigated the Breach. Instead, Filters Fast kept its website online and in full operation. As a result, unaware customers continued to shop on Defendant's compromised website for another five months.

6. Filters Fast chose to complete its internal investigation and develop a response rather than provide its customers with the information they needed to protect themselves against fraud and identity theft.

7. As alleged below, Filters Fast's failure to implement adequate data security measures for this sensitive customer information directly and proximately caused injuries to Plaintiffs and the Class (defined below).

8. The Data Breach was the inevitable result of Filters Fast's inadequate and negligent data security measures and irresponsible approach to data security. Despite the well-publicized and ever-growing threat of security breaches involving payment card networks and systems, and despite the fact that these types of data breaches were and are occurring throughout the online retail industry, Filters Fast failed to ensure that it maintained adequate data security measures, causing customer Payment Data to be stolen.

9. As a direct and proximate consequence of Filters Fast's conduct and data security shortcomings, a massive amount of customer information was stolen from Filters Fast and exposed

to criminals. Filters Fast averages approximately 574,190 website visitors each month.[1] It is predicted by SimilarWeb, a website traffic data tracker, that over 3.4 million customers shopped on the Filters Fast website from February through July 2020, putting each of these customers at an imminent and substantial risk of data theft since, throughout that timeframe, Filters Fast was fully aware of the then-unresolved Data Breach.[2]

10. Thus, millions of customers (i) had their Payment Data compromised and their privacy rights violated, (ii) were exposed to the increased and substantial risk of fraud and identify theft, (iii) lost control over their personal and financial information, and (iv) were otherwise injured.

11. Moreover, Plaintiffs and Class members have been forced to spend significant time associated with, among other things, closing out and opening new credit or debit card accounts, ordering replacement cards, obtaining fraud monitoring services, losing access to cash flow and credit lines, monitoring credit reports and accounts, and/or other losses resulting from the unauthorized use of their cards or accounts.

12. Plaintiffs and Class members seek to recover damages caused by Filters Fast's negligence, negligence *per se*, breach of contract, and violations of state consumer protection statutes. Additionally, Plaintiffs seek declaratory relief as a result of the conduct of Filters Fast discussed herein.

PARTIES

A. Plaintiff Sanger Powers

13. Plaintiff Sanger Powers ("Powers") is a citizen of the state of Wisconsin.

---

[1] *See* https://www.rapidspike.com/blog/filters-fast-allowed-3-4-million-customers-to-shop-on-hacked-site/ (last accessed September 2, 2020).
[2] *Id.*

14. During the time period when the Data Breach was occurring, Powers used a payment card to make a purchase from Filters Fast. The purchase was made on Filters Fast's website on February 4, 2020.

15. Defendant delayed until August 24, 2020 before sending a letter to Powers notifying him that his debit card was affected by the Data Breach. *See* **Exhibit 2**.

16. On August 28, Powers had four pending fraudulent charges to his affected credit card, has had to replace said credit card, and has spent hours of his time vigilantly reviewing statements and credit reports in order to contest fraudulent activity related to his compromised card. His card replacement took seven to ten days to arrive and, as such, Powers was unable to use this card for this period of time.

17. Had Powers known that Filters Fast would not adequately protect his card information and other sensitive information entrusted to it, he would not have made any purchases on the Filters Fast website.

18. As a result of Filters Fast's failure to adequately safeguard Plaintiff Powers' personal information, including payment card data, he has been injured.

B. Plaintiff Robert Legg

19. Plaintiff Robert Legg ("Legg") is a citizen of the state of Maryland.

20. During the time period when the Data Breach was occurring, Legg used a payment card to make a purchase from Filters Fast. The purchase was made on Filters Fast's website on December 4, 2019.

21. Defendant delayed until August 14, 2020 before sending a letter to Legg notifying him that his debit card was affected by the Data Breach. *See* **Exhibit 1**.

22. Plaintiff Legg has spent numerous hours responding to the Data Breach. In

particular, Legg has spent hours reviewing bank statements for charges, reviewing email scam attempts, following up and otherwise responding to the data breach trying to protect himself.

23. Because of the lost trust in Filters Fast, and because of the time he has already spent responding to and attempting to mitigate the effects of the Data Breach, Legg believes Filters Fast should do whatever it takes to make him and all others like him whole, and to take steps—enforceable by the Court—to improve its cyber security measures to prevent this from ever happening again, as well as providing a long-term credit monitoring service that will help mitigate the damage to him.

24. Had Legg known that Filters Fast would not adequately protect his card information and other sensitive information entrusted to it, he would not have made any purchases on the Filters Fast website using his payment card.

25. As a result of Filters Fast's failure to adequately safeguard Plaintiff Legg's personal information, including payment card data, Plaintiff Legg is at substantial risk of harm, including theft of his Payment Data.

C. Defendant Filters Fast, LLC

26. Filters Fast is a foreign limited liability company. It was organized in Charlotte, North Carolina and maintains its principal place of business at 5905 Stockbridge Dr., Monroe, North Carolina, 28110.

27. Through its website, Defendant Filters Fast sells a variety of filtration products, including refrigerator water filters, furnace air filters, water filtration systems, shower filters, pool and spa filters, and air purifiers.

28. Defendant touts itself as being the "#1 Online filtration retailer in the US."[3]

[3] *See* https://www.filtersfast.com/?gclid=EAIaIQobChMIy6Xxs_XK6wIVCr3ACh3nDwtyEAAYASAAEgITkfD_BwE

29. Filters Fast also sells filters globally.

JURISDICTION AND VENUE

30. This Court has subject matter jurisdiction pursuant to 28 U.S.C. § 1332, as amended by the Class Action Fairness Act of 2005, because the matter in controversy exceeds $5 million, exclusive of interest and costs, and is a class action in which some members of the Class are citizens of states different than Filters Fast. *See* 28 U.S.C. § 1332(d)(2)(A). This Court also has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367.

31. This Court has personal jurisdiction over Filters Fast because Filters Fast purposefully availed itself of the privilege of conducting business in Wisconsin; because it transacts business and supplies goods in Wisconsin; because many of the acts, claims, and omissions giving rise to this action occurred in the state of Wisconsin. Filters Fast has sufficient minimum contacts with the state of Wisconsin and intentionally availed itself, and continues to avail itself, of the jurisdiction of this Court through its business ventures, specifically through the promotion, sale, and distribution of Filters Fast products in this state, as well as through online advertising and marketing and business targeted at Wisconsin residents.

32. Venue properly lies in this district pursuant to 28 U.S.C. § 1391(a)(2) because a substantial part of the events and/or omissions giving rise to the claims asserted herein occurred in this district as Defendant conducts business throughout this district (including the promotion, sale, marketing, and distribution of its products).

FACTUAL ALLEGATIONS

A. The Data Breach

33. On or about August 14, 2020, Filters Fast confirmed in a Notice of Data Breach

(last accessed September 2, 2020).

(the "Notice") sent to Plaintiffs and Class members that Filters Fast had been made aware of a data breach that compromised customers' sensitive Payment Data. *See* Exhibit 1 and Exhibit 2, hereto (Notice Letters sent to Robert Legg and Sanger Powers).

34. The Notice provides the following, in relevant part:

> **What Happened**
>
> In late February 2020, we were informed of a possible data security incident affecting our website. We immediately began investigating the potential issue. Our investigation included hiring an outside, expert forensics firm to analyze our systems and determine if there was a breach of our security. On July 20, 2020, that investigation revealed that attackers had succeeded in adding malicious code to our website on July 15, 2019, which allowed unauthorized individuals to capture certain information during the checkout process. We removed that malicious code on July 10, 2020, during an unrelated update of our website ending the unauthorized access to our website.
>
> **What Information Was Involved?**
>
> On July 20, 2020, we confirmed the possibility that unauthorized individuals may have gained access to your name, shipping and billing address, and the payment card information used to make your purchase on FiltersFast.com.
>
> ***
>
> **What You Can Do**
>
> Please note the following:
>
> - You have zero liability for any purchases that you didn't make.
> - Monitor the payment card account used to make your purchase from FiltersFast.com.
> - Notify your payment card provider immediately if you notice any suspicious activity.
> - Be wary of telephone or email scams.

35. After nearly six months of delay, from February to August 2020, Filters Fast began sending thousands of data breach notices similar to the Notices above received by Plaintiffs, announcing the details of the Data Breach.

36. The Notice makes clear that the malicious code used to capture Plaintiffs' and Class members' personal and Payment Data was removed through an unrelated update of Filters First's website, ending the unauthorized access to the website.

37. Filters Fast disclosed in the Notice that it was made aware of the Data Breach in late February 2020, and that the hackers succeeded in carrying out a cyberattack on Filters Fast's website beginning on July 15, 2019. According to the Notice, this attack was carried out with the use of malware designed to access personal information and payment card data from information provided on Defendant's website.

38. However, despite being notified in February 2020 that malicious code was present on its website, Defendant did not take the website offline while it investigated the Data Breach. Instead, Filters Fast chose to prioritize its profits above the security of its customers' information by allowing its website to remain online and fully operational.

39. Additionally, on its checkout page, Filters Fast places a "Privacy Guaranteed" message, further inducing customers to trust Filters Fast with their Payment Data and other personal information.

40. These decisions left millions of unaware customers exposed to the imminent and substantial risks inherent in a data breach, including the compromise and fraudulent use of their personal and Payment Data.

41. According to Filters Fast, the Data Breach exposed the Payment Data of approximately 323,000 individuals.[4]

42. Members of the Class have already experienced fraudulent activity, including

[4] *See* Indiana's Attorney General website, available at: https://www.in.gov/attorneygeneral/files/data%20breach%20sept2020.pdf.

unauthorized purchases on their compromised debit and credit cards.[5]

B. Filters Fast Failed to Adequately Protect Its Customers' Payment Data

43. It is well known that sensitive Payment Data is valuable and frequently targeted by hackers. In a recent article, Business Insider noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. At least 11 consumer companies reported data breaches in the last year. Many of them were caused by flaws in payment systems either online or in stores."[6]

44. As is commonplace with payment card data breaches, the Filters Fast Data Breach was a result of an approach routinely used by cybercriminals referred to as "web skimming," in which a malicious code is entered into the ecommerce website in an effort to capture customers' personal and financial data.

45. Ensighten, a global cybersecurity leader providing client-side protection against data loss, ad injection and intrusion, explains the recent surge in website skimming and data theft as follows:

> [D]ue to the move to more secure chip-based card infrastructure, it is becoming more expensive for thieves to fabricate and successfully use stolen customer data. As such, criminals are now turning their attention to website skimming, with ecommerce website attacks described as "off the charts" over the past year. A Symantec report shows that an average of 4,800 websites are compromised … each month.[7]

46. Despite the known risk of a data breach and the widespread publicity and industry alerts regarding the other notable data breaches, Filters Fast failed to take reasonable steps to adequately protect its computer systems from being breached, and then failed to detect the Data

[5] *See* August 19, 2020 review by Janet Boggs (https://www.trustpilot.com/review/www.filtersfast.com?page=3&stars=1) (last accessed September 2, 2020).
[6] Dennis Green & Mary Hanbury, "If you bought anything from these 11 companies in the last year, your data may have been stolen," BUSINESS INSIDER (Aug. 15, 2019), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.
[7] *See* https://www.ensighten.com/blog/how-an-online-skimming-attack-unfolds (last accessed September 2, 2020).

Breach for several months.

47. Then, even after detecting the malicious code on its website, Filters Fast failed to take its website offline. Instead, Filters Fast allowed its customers to continue shopping and submitting their personal information and Payment Data to a website that was compromised, without making any effort to minimize Plaintiffs' and Class members' exposure. In fact, Filters Fast continued to include a "Privacy Guaranteed" message on its website's checkout page.

48. Filters Fast is, and at all relevant times has been, aware that the Payment Data it maintains as a result of purchases made on its website is highly sensitive and could be used for nefarious purposes by third parties, such as perpetrating identity theft and making fraudulent purchases.

49. Filters Fast's motto, "Filter. Purify. Protect.", also included on the compromised website during the time of the Data Breach, makes clear that Filters Fast recognizes the importance of adequately safeguarding its customers' sensitive Payment Data.

50. Filters Fast, which conducts its ecommerce business through its website, is aware of the importance of safeguarding its customers' Payment Data from the foreseeable consequences that would occur if its data security systems were breached. This is evident from Defendant's own Privacy Policy within its Terms and Conditions, which states:

> **Information Collection, Use, and Sharing**
>
> Here at FiltersFast.com - ***we take your privacy seriously as it is important to us.*** This privacy statement explains what personal data we collect from you, and how it is used and shared. Also outlined in this policy is how you can control the collection of, make corrections to, and/or request the deletion of information.
>
> We will not use or share your information with anyone except as described in this Privacy Policy, and we will never sell or rent this information to anyone.
>
> ***
>
> **Security**

> We take precautions to protect your information. ***When you submit sensitive information via the website, your information is protected both online and offline.***
>
> ***Sensitive information, such as credit card data, that is collected is encrypted and transmitted to us in a secure way.*** You can verify this by looking for a closed lock icon at the bottom of your web browser or looking for "https" at the beginning of the address of the web page.
>
> ***While we use encryption to protect sensitive information transmitted online, we also protect your Information offline. Only employees who need the information to perform a specific job (for example, billing or customer service) are granted access to personally identifiable information.*** The computers/servers in which we store personally identifiable information are kept in a secure environment here in the USA.
>
> [Emphasis added.[8]]

51. Financial institutions and credit card processing companies have issued rules and standards governing the basic measures that merchants must take to ensure that consumers' valuable data is protected.

52. 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 online merchants like Filters Fast 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.

53. The twelve requirements of the PCI DSS are:

1. Install and maintain a firewall configuration to protect cardholder data;
2. Do not use vendor-supplied defaults for system passwords and other security parameters;

[8] *See* https://www.filtersfast.com/termsAndCond.asp.

3. Protect stored cardholder data;
4. Encrypt transmission of cardholder data across open, public networks;
5. Protect all systems against malware and regularly update anti-virus software or programs;
6. Develop and maintain secure systems and applications;
7. Restrict access to cardholder data by business need to know;
8. Identify and authenticate access to system components;
9. Restrict physical access to cardholder data;
10. Track and monitor all access to network resources and cardholder data;
11. Regularly test security systems and processes; and
12. Maintain a policy that addresses information security for all personnel.[9]

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

55. Filters Fast was always fully aware of its data protection obligations in light of its participation in its online payment card processing system's collection and transmission of thousands of sets of Payment Data.

56. Because Filters Fast accepted payment cards containing sensitive financial information, it knew that its customers were entitled to and did in fact rely on it to keep that sensitive information secure from would-be data thieves in accordance with the PCI DSS requirements. Nevertheless, Filters Fast did not adhere to the PCI DSS requirements.

57. 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); *In re BJ's Wholesale Club, LLC*, 140 F.T.C. 465 (2005).

[9]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.

58. In 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 consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone may be trying to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

59. The FTC has also published a document, entitled "Protecting Personal Information: A Guide for Business," which highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[10]

60. The FTC has issued orders against businesses that failed to employ reasonable measures to secure Payment Data. These orders provide further guidance to businesses in regard to their data security obligations.

61. As noted above, Filters Fast should have been and, based upon its notification in February 2020 of malicious code on its website, *was* aware of the need to have adequate, updated data security systems in place.

62. Despite this, Filters Fast failed to update and maintain its data security systems in a meaningful way so as to prevent data breaches. Filters Fast's security flaws run afoul of industry best practices and standards. More specifically, the security practices in place at Filters

[10]FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited November 8, 2019).

Fast are in stark contrast and directly conflict with the PCI DSS core security standards.

63. Had Filters Fast maintained its information technology systems ("IT systems"), adequately protected them, and had adequate security safeguards in place, it could have prevented the Data Breach.

64. As a result of industry warnings, awareness of industry best practices, the PCI DSS, and numerous well-documented restaurant, retail, and e-commerce data breaches, Filters Fast was alerted to the risk associated with failing to ensure that its IT systems were adequately secured. Filters Fast was not only aware of the threat of data breaches, generally, but was aware of the specific danger of malware infiltration. Malware has been used recently to infiltrate large retailers such as, *inter alia*, Target, GameStop, Chipotle, Jason's Deli, Whole Foods, Sally Beauty, Neiman Marcus, Michaels Stores, and Supervalu. As a result, Filters Fast was aware that malware is a real threat and is a primary tool of infiltration used by hackers.

65. In addition to the publicly announced data breaches described above, Filters Fast knew or should have known of additional warnings regarding malware infiltrations from the U.S. Computer Emergency Readiness Team, a government unit within the Department of Homeland Security, which alerted retailers to the threat of malware on July 31, 2014, and issued a guide for retailers on protecting against the threat of malware, which was updated on August 27, 2014.[11]

66. Despite the fact that Filters Fast was on notice of the very real possibility of consumer data theft associated with its security practices and that Filters Fast knew or should have known about the elementary infirmities associated with its security systems, it still failed to make necessary changes to its security practices and protocols, and permitted massive

[11] *See* U.S. COMPUTER EMERGENCY READINESS TEAM, "Alert (TA14-212A): Backoff Point-of-Sale Malware," (July 31, 2014) (revised Sept. 30, 2016), https://www.us-cert.gov/ncas/alerts/TA14-212A.

malware intrusions to occur for months on end without notifying Plaintiffs and Class members.

67. Moreover, Filters Fast was *specifically* made aware of the fact that malicious code had been placed on its website in February 2020. It was not until July 2020 that Filters Fast removed this malicious code. Thus, Defendant allowed its *knowingly* unsecure website to remain online and to accept Payment Data from at least February 2020 through July 2020.

68. Filters Fast, at all times relevant to this action, had a duty to Plaintiffs and members of the Class to: (a) properly secure Payment Data submitted to or collected Filters Fast's website; (b) encrypt Payment Data using industry standard methods; (c) use available technology to defend its system from well-known methods of invasion; (d) act reasonably to prevent the foreseeable harms to Plaintiffs and the Class that would naturally result from Payment Data theft; and (e) promptly notify customers when Filters Fast became aware of the potential that customers' Payment Data would be compromised.

69. Defendant failed in all the aforementioned obligations. Instead, Filters Fast permitted customers' Payment Data to be compromised by failing to take reasonable steps against an obvious threat.

70. In addition, leading up to the Data Breach, and during the Breach itself and the investigation that followed, Filters Fast failed to follow the guidelines set forth by the FTC.

71. Industry experts are clear that a data breach is indicative of data security failures. Indeed, Julie Conroy—research director at the research and advisory firm Aite Group—has identified that, "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[12]

72. The Data Breach is particularly egregious and its data security failures are

[12]Lisa Baertlein, "Chipotle Says Hackers Hit Most Restaurants in Data Breach," REUTERS (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY.

alarming given that the Breach resulted in potentially millions of cards being stolen and illegally placed for sale on the dark web, and because it was permitted to occur for over a year (6 months of which Filters Fast knew and refused to notify Plaintiffs and the Class).

73. Clearly, had Filters Fast utilized adequate data security and data breach precautions and response protocols, the window of the Data Breach would have been significantly mitigated, and the level of impact could have been reduced (or not permitted to happen in the first place).

74. Due to Defendant's inadequate security and failure to remediate the problem in a timely manner, Filters Fast's customers' Payment Data is now in the hands of cybercriminals who can quickly turn a profit by posting the Payment Data on the dark web. As one data security commentator noted in response to an unrelated data breach:

> . . . ***2 million cards on sale on the dark web would indicate this was a very successful project for the cybercriminals involved, and one which is likely to be incredibly profitable***. . . .[13]

75. With likely millions of cards stolen in the Filters Fast breach, this clearly marks a highly successful outing for criminals and a large failure on Filters Fast's part as to data security.

76. As a result of the events detailed herein, Plaintiffs and members of the Class suffered actual, palpable fraud and losses resulting from the Data Breach, including financial losses related to the purchases made at Filters Fast that Plaintiffs and Class members would not have made had they known of Filters Fast's careless approach to cybersecurity; lost control over the value of personal information and Payment Data, for which personal information and Payment Data there is a well-established and quantifiable national and international market; loss of time and money expended in responding to the Data Breach and attempting to mitigate the harms of

[13]"Cyber Attack on Earl Enterprises (Planet Hollywood)," is Buzznews (Apr. 1, 2019), https://www.informationsecuritybuzz.com/expert-comments/cyber-attack-on-earl-enterprises- planet-hollywood/.

the Data Breach; loss of time and money resolving fraudulent charges and obtaining new debit and/or credit cards; loss of time obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Payment Data.

77. These costs and expenses will continue to accrue as additional fraud alerts and fraudulent charges occur and are discovered.

78. For example, the Payment Data stolen from Filters Fast's website can be used to drain debit card-linked bank accounts, make "clone" credit cards, or to buy items on certain less-secure websites. To date, Filters Fast is not taking any real measures to assist affected customers other than providing a woefully inadequate 12 months of free credit monitoring.

79. Defendant has only slowly provided information about the Data Breach at its own pace over the course of six months, leaving victims of the Data Breach in the dark and vulnerable to continued fraud.

80. Filters Fast's failure to adequately protect its customers' Payment Data resulted in consumers having to expend extensive amounts of time, calls, and, for many of the credit and fraud protection services, payment of their own money—while Filters Fast did little to assist those affected by the Data Breach, and withholding important details about the Data Breach as it conducts its investigation.

CLASS ALLEGATIONS

81. Plaintiffs bring this action individually and on behalf of the following Class and Subclass pursuant to FED. R. CIV. P. 23:

> **The Nationwide Class**
> All individuals in the United States who had their credit or debit Payment Data compromised as a result of the Filters Fast data breach (the "Nationwide Class").
>
> **The Wisconsin Subclass**
> All individuals in the State of Wisconsin who had their credit or debit Payment Data compromised as a result of the Filters Fast data breach (the "WI Subclass").

The Maryland Subclass

> All individuals in the State of Maryland who had their credit or debit Payment Data compromised as a result of the Filters Fast data breach (the "MD Subclass").

82. Excluded from the Nationwide Class and MD and WI Subclasses are Filters Fast, its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case.

83. Plaintiffs reserve the right to modify, change, or expand the definition of the Nationwide Class, WI Subclass, and MD Subclass, or to propose alternative or additional subclasses based on discovery and further investigation.

84. The Nationwide Class and the WI and MD Subclasses are collectively referred to throughout this Complaint as the "Class," unless otherwise specified.

85. **Numerosity**: While the precise number of Class members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include approximately 323,000 members who are geographically dispersed. Upon information and belief, the Data Breach affected millions of Filters Fast consumers across the United States.

86. **Typicality**: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through Filters Fast's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their sensitive data and Payment Data compromised in the same way by the same conduct by Filters Fast.

87. **Adequacy**: Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the Class that they seek to represent; Plaintiffs have retained counsel competent and highly experienced in Class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be

fairly and adequately protected by Plaintiffs and their counsel.

88. **Superiority**: A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs 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 very difficult if not impossible for members of the Class individually to effectively redress Filters Fast's 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 the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

89. **Existence and Predominance of Common Questions of Fact and Law:** Common questions of law and fact exist as to Plaintiffs and all members of the Class. These questions predominate over the questions affecting individual Class members. These common legal and factual questions include, but are not limited to, the following:

- whether Filters Fast engaged in the wrongful conduct alleged herein;
- whether Filters Fast owed a duty to Plaintiffs and members of the Class to adequately protect their Payment Data and to provide timely and accurate notice of the Data Breach to Plaintiffs and the Class, and whether it breached these duties;
- whether Filters Fast violated federal and state laws thereby breaching its duties to Plaintiffs and the Class as a result of the Data Breach;
- whether Filters Fast knew or should have known that its website was vulnerable to

attacks from hackers and cyber-criminals;

- whether Filters Fast's conduct, including its failure to act, resulted in or was the proximate cause of the Breach of its website resulting in the theft of customers' Payment Data;
- whether Filters Fast wrongfully failed to inform Plaintiffs and members of the Class that it did not maintain website and other security procedures and precautions sufficient to reasonably safeguard consumers' sensitive financial and personal data;
- whether Filters Fast failed to inform Plaintiffs and the Class of the Data Breach in a timely and accurate manner;
- whether Filters Fast continues to breach duties to Plaintiffs and Class;
- whether Filters Fast has sufficiently addressed, remedied, or protected Plaintiffs and Class members following the Data Breach and has taken adequate preventive and precautionary measures to ensure the Plaintiffs and Class members will not experience further harm;
- whether Plaintiffs and members of the Class suffered injury as a proximate result of Filters Fast's conduct or failure to act; and
- whether Plaintiffs and the Class are entitled to recover damages, equitable relief, and other relief, and the extent of the remedies that should be afforded to Plaintiffs and the Class.

90. Filters Fast has acted or refused to act on grounds generally applicable to Plaintiffs and the other members of the Class, thereby making appropriate final injunctive relief and declaratory relief with respect to the Class as a whole.

91. Given that Filters Fast has engaged in a common course of conduct as to Plaintiffs

and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions far outweigh any potential individual questions.

92. The Class is defined in terms of objective characteristics and common transactional facts, namely, the exposure of sensitive Payment Data to cyber criminals due to Filters Fast's failure to protect this information, adequately warn the Class that it lacked adequate data security measures, and failure to adequately warn that it was breached. Class membership will be readily ascertainable from Filters Fast's business records.

93. Plaintiffs reserve the right to revise the above Class definitions and any of the averments of fact herein based on facts adduced in discovery.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, Each Subclass)

94. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

95. Filters Fast collected Payment Data from Plaintiffs and Class members in exchange for its sale of filtration products on its website.

96. Filters Fast owed a duty to Plaintiffs and the Class to maintain confidentiality and to exercise reasonable care in safeguarding and protecting their financial and personal information, in Filters Fast's possession, from being compromised by unauthorized persons. This duty included, among other things, designing, maintaining, and testing Filters Fast's website, networks and data security systems to ensure that Plaintiffs' and Class members' financial and personal information in Filters Fast's possession was adequately protected in the process of collection and following collection while stored on Filters Fast's systems.

97. Filters Fast further owed a duty to Plaintiffs and Class members to implement

processes that would detect a breach of its website and security system in a timely manner and to timely act upon warnings and alerts, including those generated by its own security system.

98. Filters Fast owed a duty to Plaintiffs 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 Plaintiffs and Class members whose confidential data Filters Fast obtained and maintained.

99. Filters Fast knew, or should have known, of the risks inherent in collecting and storing the financial and personal information of Plaintiffs and Class members and of the critical importance of providing adequate security for that information.

100. Filters Fast's conduct created a foreseeable risk of harm to Plaintiffs and members of the Class. This conduct included but was not limited to Filters Fast's failure to take the steps and opportunities to prevent and stop the Data Breach as described herein. Filters Fast's conduct also included its decision not to comply with industry standards for the safekeeping and maintenance of the financial and personal information of Plaintiffs and Class members.

101. Filters Fast knew or should have known that it had inadequate computer systems and data security practices to safeguard such information, and Filters Fast knew or should have known that hackers would attempt or were attempting to access the personal financial information in Filters Fast's systems.

102. Filters Fast breached the duties it owed to Plaintiffs and members of the Class by failing to exercise reasonable care and implement adequate security systems, protocols, and practices sufficient to protect the financial and personal information of Plaintiffs and members of the Class, as identified above. This breach was a proximate cause of injuries and damages suffered

by Plaintiffs and Class members.

103. As a direct and proximate result of Filters Fast's negligent conduct, Plaintiffs and Class members have been injured and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, Each Subclass)

104. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

105. Pursuant to the FTC Act, 15 U.S.C. § 45, Filters Fast had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' personal information.

106. 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, such as Filters Fast, of failing to use reasonable measures to protect Payment Data. The FTC publications and orders described above also form part of the basis of Filters Fast's duty to protect Plaintiffs' and Class members' sensitive information.

107. Filters Fast violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect Payment Data and not complying with applicable industry standards, including PCI DSS, as described in detail herein. Filters Fast's conduct was particularly unreasonable given the nature and amount of Payment Data it collected and stored and the foreseeable consequences of a data breach, including, specifically, the immense damages that would result to consumers and financial institutions.

108. The harm that has occurred is the type of harm the FTC Act (and similar state statutes) is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions

against businesses that, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

109. Filters Fast had a duty to Plaintiffs and Class members to implement and maintain reasonable security procedures and practices to safeguard Plaintiffs' and Class members' personal information.

110. Filters Fast breached its duties to Plaintiffs and Class members under the FTC Act (and similar state statutes), by failing to provide fair, reasonable, or adequate website and data security practices to safeguard Plaintiffs' and Class members' financial and personal information.

111. Filters Fast's violation of Section 5 of the FTC Act (and similar state statutes) and its failure to comply with applicable laws and regulations constitutes negligence *per se*.

112. But for Filters Fast's wrongful and negligent breach of its duties owed to Plaintiffs and Class members, they would not have been injured.

113. The injury and harm suffered by Plaintiffs and Class members was the reasonably foreseeable result of Filters Fast's breach of its duties. Filters Fast knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and Class members to suffer the foreseeable harms associated with the exposure of their Payment Data.

114. Had Plaintiffs and Class members known that Filters Fast did and does not adequately protect customer Payment Data, and that Filters Fast's website was compromised during the months they made their purchases, they would not have made the purchases.

115. As a direct and proximate result of Filters Fast's negligence *per se*, Plaintiffs and Class members have suffered harm, including but not limited to, loss of time and money responding to the Data Breach, including resolving fraudulent charges, obtaining protection

against future identity theft, and otherwise mitigating the harms caused by the Breach; financial losses related to the purchases made at Filters Fast that Plaintiffs and Class members would not have made had they known of the Data Breach and Filters Fast's careless approach to cyber security and responding to the Breach; lost control over the value of personal information; and other harm resulting from the unauthorized use or threat of unauthorized use of stolen Payment Data, entitling them to damages in an amount to be proven at trial.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, Each Subclass)

116. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

117. Plaintiffs and Class members who made purchases on Filters Fast's website during the period in which the Data Breach occurred had implied contracts with Filters Fast.

118. Specifically, Plaintiffs and Class members paid money to Filters Fast and, in connection with those transactions, provided Filters Fast with their Payment Data. In exchange, Filters Fast agreed, among other things: (1) to provide the filter product(s) being purchased; (2) to take reasonable measures to protect the security and confidentiality of Plaintiffs' and Class members' Payment Data; and (3) to protect Plaintiffs' and Class members' personal information in compliance with federal and state laws and regulations and industry standards.

119. Protection of personal information is a material term of the implied contracts between Plaintiffs and Class members and Filters Fast. Indeed, as described above, Filters Fast recognized the importance of data security and privacy of customers' sensitive financial information. Had Plaintiffs and Class members known that Filters Fast would not adequately protect their Payment Data, or that Filters Fast's website was breached, they would not have made

purchases on Filters Fast's website.

120. Filters Fast did not satisfy these agreements and obligations to Plaintiffs and Class members under the implied contracts because it did not take reasonable measures to keep their personal information secure and confidential, and because it did not comply with applicable laws, regulations, and industry standards.

121. Filters Fast materially breached its implied contracts with Plaintiffs and Class members by failing to implement adequate Payment Data security measures.

122. Plaintiffs and Class members fully performed their obligations under their implied contracts with Filters Fast.

123. Filters Fast's failure to satisfy its obligations led directly to the successful intrusion of Filters Fast's website and to the unauthorized parties' access and exfiltration of Plaintiffs' and Class members' Payment Data.

124. Filters Fast breached these implied contracts as a result of its failure to implement security measures adequate to protect Plaintiffs' and Class members' Payment Data.

125. Also, as a result of Filters Fast's failure to implement proper security measures, Plaintiffs and Class members suffered actual damages resulting from the compromise of their personal information and remain at an imminent and substantial risk of suffering additional damages in the future.

126. Accordingly, Plaintiffs and Class members have been injured as a proximate result of Filters Fast's breach of implied contracts and are entitled to damages and/or restitution in an amount to be proven at trial.

COUNT IV
Violation of the Wisconsin's Deceptive Trade Practices Act
WIS. STAT. § 100.18 ("WDTPA")
(On Behalf of Plaintiff Powers and the WI Subclass)

127. Plaintiff Powers realleges and incorporates all previous allegations as though fully set forth herein.

128. Wisconsin's Deceptive Trade Practices Act, Wis. Stat. § 100.18(1) (the "WDTPA"), establishes the following:

> "No … corporation … or agent or employee thereof, with intent to sell, distribute, increase the consumption of or in any wise dispose of any … merchandise … to the public for sale … or with intent to induce the public in any manner to enter into any contract or obligation relating to the purchase … of any … merchandise … shall make, publish, disseminate, circulate, or place before the public, or cause, directly or indirectly, to be made, published, disseminated, circulated, or placed before the public, in this state, in a newspaper, magazine or other publication, or in the form of a book, notice, handbill, poster, bill, circular, pamphlet, letter, sign, placard, card, label, or over any radio or television station, or in any other way similar or dissimilar to the foregoing, an advertisement, announcement, statement or representation of any kind to the public relating to such purchase, sale, … or lease of such real estate, merchandise, securities, service or employment or to the terms or conditions thereof, which advertisement, announcement, statement or representation contains any assertion, representation or statement of fact which is untrue, deceptive or misleading."

!

129. By reason of the conduct alleged herein, and by failing to provide reasonable security measures for the protection of the Payment Data of Powers and WI Subclass members, Filters Fast engaged in practices generally prohibited under Wis. Stat. § 100.18(1).

130. Filters Fast's conduct as set forth herein constitutes a fraudulent representation including, but not limited to, Filters Fast's "Privacy Guaranteed" representation and security representations made in Defendant's Privacy Policy on its website, to Powers and all WI Subclass members, along with its known concealment, suppression and omission of material facts relating to the Data Breach, with the intent that Powers and members of the WI Subclass relied on the same in connection with Filters Fast's promotion and sale of consumer goods on its website.[14]

[14] While omissions alone are not actionable under the WDTPA, "[a] nondisclosure of facts, combined with an affirmative representation that is undermined by the non-disclosed facts, may result in liability under § 100.18(1)."

131. Filters Fast's fraudulent practices, including the "Privacy Guaranteed" message on the checkout page of its website and the Privacy Policy on its website, along with its known concealment, suppression and omission of material facts relating to the Data Breach, materially induced Powers and other members of the WI Subclass to pay more than they otherwise would have paid (if at all) had they known the website was likely breached and that their Payment Data was at risk of being compromised.

132. These fraudulent practices caused Powers and WI Subclass members to suffer losses as set forth and alleged herein.

133. Filters Fast had a duty to disclose to Powers and members of the WI Subclass that it did not and could not adequately protect or "guarantee privacy" of sensitive Payment Data and personal information, as these facts were material to Powers' and WI Subclass members' transactions; Filters Fast, as the party with knowledge of its data security shortcomings, knew that Powers and members of the WI Subclass were entering transactions under a mistake as to the fact of its data security practice and should have protected them accordingly.

134. Due to the Data Breach, Powers and WI Subclass members have lost property in the form of their Payment Data and have suffered actual damages. Further, Filters Fast's failure to adopt reasonable practices in protecting and safeguarding the confidential and sensitive financial information of its customers has resulted in Powers and WI Subclass members spending time monitoring their accounts.

135. Powers and WI Subclass members are now at a higher and more substantial risk of identity theft crimes. This harm sufficiently outweighs any justifications or motives for Filters

---

Christensen v. TDS Metrocom LLC, 2009 WI App 21, 316 Wis. 2d 356 n.4, 763 N.W.2d 248. Here, Filters Fast's "Privacy Guaranteed" representation and security representations made in Defendant's Privacy Policy on its website, are affirmative misrepresentations, not omissions.

Fast's practice of leaving its website online in the middle of a known Data Breach while continuing to expose confidential and sensitive financial information without the appropriate and reasonable safeguards to protect such information.

136. As a result of Filters Fast's practices, acts and omission, in violation of the WAFTPA, Powers and WI Subclass members have suffered injury-in-fact and have lost money or property. As a result of Filters Fast's failure to adopt, implement, and maintain reasonable security procedures, and the resulting Data Breach, Powers and WI Subclass members have incurred costs and spent time associated with monitoring and repairing their credit and issues of identity theft.

137. Filters Fast's conduct proximately caused the injuries to Powers and WI Subclass members and they are entitled to all damages, in addition to costs, interest and fees, including attorneys' fees, as allowed by law.

COUNT V
Violation of the Maryland Consumer Protection Act
MD CODE ANN., COM. LAW § 13-301, et seq. ("MDTPA")
(On Behalf of Plaintiff Legg and the MD Subclass)

138. Plaintiff Legg realleges and incorporates all previous allegations as though fully set forth herein.

139. Section 13-301 of the Maryland Consumer Protection Act defines an unfair or deceptive trade practice, in relevant part, as the following:

> "Deception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that a consumer rely on the same in connection with (i) The promotion or sale of any consumer goods, consumer realty, or consumer service…" Md. Code Ann., Com. Law § 13-301(9)(i).

!

140. Section 13-302 establishes that any prohibited practice under § 13-303 "is a violation of this title, whether or not any consumer in fact has been misled, deceived, or damaged as a result of that practice."

141. By reason of the conduct alleged herein, and by failing to provide reasonable security measures for the protection of the Payment Data of Legg and MD Subclass members, Filters Fast engaged in practices generally prohibited under Md. Code Ann., Com. Law § 13-303.

142. Filters Fast's conduct as set forth herein constitutes unfair or deceptive acts or practices, including, but not limited to, its known concealment, suppression and omission of material facts relating to the Data Breach with the intent that Legg and members of the MD Subclass relied on the same in connection with Filters Fast's promotion and sale of consumer goods on its website.

143. Filters Fast's unfair and deceptive practices, including the "Privacy Guaranteed" message on the checkout page of its website and the security representations within the Privacy Policy on its website, along with its known concealment, suppression and omission of material facts relating to the Data Breach, and its initial omissions concerning its data security, materially induced Legg and other members of the MD Subclass to pay more than they otherwise would have paid (if at all) had they known the website was likely breached and that their Payment Data was at risk of being compromised.

144. These deceptive practices caused Legg and MD Subclass members to suffer losses as set forth herein.

145. Filters Fast had a duty to disclose to Legg and members of the MD Subclass that it did not and could not adequately protect sensitive Payment Data, as the facts were contrary to representations in Defendant's Privacy Policy and since such facts were material to Legg's and MD Subclass members' transactions. Filters Fast, as the party with knowledge of its data security shortcomings, knew that Legg and members of the MD Subclass were entering transactions under a mistake as to the fact of its data security practice and should have protected them accordingly.

146. Due to the Data Breach, Legg and MD Subclass members have lost property in the form of their Payment Data and have suffered actual damages. Further, Filters Fast's failure to adopt reasonable practices in protecting and safeguarding the confidential and sensitive financial information of its customers has resulted in Legg and MD Subclass members spending time monitoring their accounts. Legg and MD Subclass members are now at a higher and more substantial risk of identity theft crimes. This harm sufficiently outweighs any justifications or motives for Filters Fast's practice of leaving its website online in the middle of a known Data Breach while continuing to expose confidential and sensitive financial information without the appropriate and reasonable safeguards to protect such information.

147. As a result of Filters Fast's practices, acts and omission, in violation of the MDTPA, Legg and MD Subclass members have suffered injury-in-fact and have lost money or property. As a result of Filters Fast's failure to adopt, implement, and maintain reasonable security procedures, and the resulting Data Breach, Legg and MD Subclass members have incurred costs and spent time associated with monitoring and repairing their credit and issues of identity theft.

148. Filters Fast's conduct proximately caused the injuries to Legg and the MD Subclass members and they are entitled to all damages, in addition to costs, interest and fees, including attorneys' fees, as allowed by law.

COUNT VI
Violation of the Maryland Personal Information Protection Act
MD CODE ANN., COM. LAW § 14-3501, et seq. ("MPIPA")
(On Behalf of Plaintiff Legg and the MD Subclass)

149. Plaintiff Legg realleges and incorporates all previous allegations as though fully set forth herein.

150. By reason of the conduct alleged herein, and by failing to provide reasonable security measures for the protection of the Payment Data of Legg and MD Subclass members,

Defendants violated the provisions of § 14-3501, et seq. of the MPIPA.

151. Legg's and MD Subclass members' Payment Data includes personal information specifically defined under § 14-3501(e)(1).

152. Legg and MD Subclass members are "customers" as defined by Section 14-3502 as individuals residing in Maryland who provide personal information to a business for the purpose of purchasing or leasing a product or obtaining a service from the business.

153. Defendant is a business, as defined under § 14-3501(b)(1), that maintains certain computerized data that includes personal information, as described in § 14-3504(b)(2), which personal information includes the Payment Data of Legg and MD Subclass members.

154. It took Defendant seven (7) months to detect the Data Breach and then, once it knew of the Data Breach and intrusion into its website and Payment Data environment, Defendant chose to leave the website online while it spent another five (5) months investigating the Data Breach, exposing its customers, including Legg and the MD Subclass, to the compromised website.

155. The five-month investigation was not a reasonable and prompt investigation as required by § 14-3504(b)(1), and Defendant delayed in sending the statutorily required notice well past the 45 days required under § 14-3504(b)(3).

156. By failing to disclose the Data Breach in a timely and accurate fashion, Legg and MD Subclass members were harmed because they were not immediately able to take action and precautions to prevent the compromise of their Payment Data.

157. Pursuant to § 14-3508, a violation of the MPIPA is an unfair or deceptive trade practice within the meaning of Title 13 of the Maryland Code, Commercial Law and is subject to the enforcement and penalty provisions contained in Title 13.

158. Under § 13-408(a) of the Maryland Commercial Code, "any person may bring an

action to recover for injury or loss sustained by him as result of a practice prohibited by this title."

159. Due to the Data Breach and Defendant's failure to disclose such to its customers, Legg and MD Subclass members have lost property in the form of their personal information and Payment Data and have suffered actual damages. Legg and MD Subclass members are now at a higher, more substantial and imminent risk of identity theft crimes. This harm sufficiently outweighs any justifications or motives for Defendant's practice of collecting and storing confidential and sensitive financial information without the appropriate and reasonable safeguards to protect such information.

160. As a result of Defendant's failure to adopt, implement, and maintain reasonable security procedures, and the resulting Data Breach, Legg and MD Subclass members have suffered injuries in fact in an amount of damages that is to be determined at trial.

COUNT VII
Unjust Enrichment
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, Each Subclass)

161. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

162. This claim is pleaded in the alternative to the above breach of implied contract claim.

163. Plaintiffs and Class members conferred a monetary benefit upon Filters Fast in the form of monies paid for the purchase of filtration products on the Filters Fast website.

164. Filters Fast had knowledge of the benefits conferred upon them by Plaintiffs and Class members. Filters Fast also benefited from the receipt of Plaintiffs' and Class members' Payment Data, as this was utilized by Filters Fast to facilitate payment to it.

165. The monies for the filtration products that Plaintiffs and Class members paid to Filters Fast were supposed to be used by Filters Fast, in part, to pay for the administrative costs of

reasonable data privacy and security practices and procedures.

166. As a result of Filters Fast's acts and omissions, Plaintiffs and Class members suffered actual damages in an amount equal to the difference in value between their purchases made with the assumption that reasonable data privacy and security practices and procedures were being paid for with Plaintiffs' and Class members' purchases, and the purchases made without actually receiving the reasonable data privacy and security practices and procedures that they believed they were paying for.

167. Under principals of equity and good conscience, Filters Fast should not be permitted to retain the money belonging to Plaintiffs and Class members because Filters Fast failed to implement (or adequately implement) the data privacy and security practices and procedures that Plaintiffs and Class members paid for and that were otherwise mandated by federal, state, and local laws and industry standards.

168. Filters Fast should be compelled to disgorge into a common fund for the benefit of Plaintiffs and Class members all unlawful or inequitable proceeds received by it as a result of the conduct and Data Breach alleged herein.

COUNT VIII
Declaratory Relief
(On Behalf of Plaintiffs and the Nationwide Class or, Alternatively, Each Subclass)

169. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

170. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

171. As previously alleged and pleaded, Defendant owes duties of care to Plaintiffs and Class members that require it to adequately secure their Payment Data.

172. Defendant still possesses the Payment Data of Plaintiffs and Class members.

173. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and Class members.

174. Upon information and belief, Defendant is only taking minimal steps to increase its data security but there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Data Breach, and to once again place profits above protection.

175. Plaintiffs and Class members therefore seek a declaration that (1) Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant to engage third-party security auditors/penetration testers, as well as internal security personnel, to conduct testing that includes simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering Defendant to significantly increase its spending on cybersecurity, including website, systems and personnel;

c. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;

d. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

e. Ordering that Defendant conduct regular database and website scanning and

securing checks;

f. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

g. Ordering Defendant to implement and enforce adequate retention policies for Payment Data, including destroying Payment Data as soon as it is no longer necessary for it to be retained.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and the Class, respectfully request that the Court grant the following relief:

A. Certify this case as a class action pursuant to FED. R. CIV. P. 23(a) and (b)(3), and, pursuant to FED. R. CIV. P. 23(g), appoint Plaintiffs as Class representatives and their counsel as Class counsel.

B. Award Plaintiffs and the Class appropriate monetary relief, including actual damages, restitution, and disgorgement.

C. Award Plaintiffs and the Class equitable, injunctive and declaratory relief as may be appropriate. Plaintiffs, on behalf of the Class, seek appropriate injunctive relief designed to protect against the recurrence of a data breach by Filters Fast's adoption and implementation of the best data security\ practices to safeguard its customers' financial and personal information, extension of adequate credit monitoring services and similar services to protect against all types of identity theft, especially including card theft and fraudulent card charges, and provision of elevated credit monitoring services to minor and elderly Class members who are more susceptible to fraud and identity theft.

D. Award Plaintiffs and the Class pre-judgment and post-judgment interest to the

maximum extent allowable.

E. Award Plaintiffs and the Class reasonable attorneys' fees and costs as allowable.

F. Award Plaintiffs and the Class such other favorable relief as allowable under law or at equity.

Dated: October 26, 2020

Respectfully submitted,

/s/ John D. Blythin
Shpetim Ademi (SBN 1026973)
John D. Blythin (SBN 1046105)
Ademi LLP
3620 East Layton Avenue
Cudahy, Wisconsin 53110
Tel: 414-482-8000
Fax: 414-482-8001
sademi@ademilaw.com
jblythin@ademilaw.com

William B. Federman,
Pro Hac Vice Pending
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
Tel: (405) 235-1560
Fax: (405) 239-2112
wbf@federmanlaw.com

Counsel for Plaintiffs Sanger Powers, Robert Legg, and the Putative Class

Exhibit 1

FILTERSFAST.COM
Filter. Purify. Protect.

C/O ID Experts
P.O. Box 6336
Portland, OR 97228-6336

0030 [redacted]8729

ROBERT LEGG
1713 LAUREL BROOK RD
FALLSTON MD 21047-2128

August 14, 2020

Notice of Data Breach

Dear Robert Legg,

At FiltersFast.com, we are dedicated to our motto to "Filter. Purify. Protect." Since our start in 2004, transparency has been a cornerstone of that commitment. It is in that spirit of transparency that I write to notify you of an incident that may have impacted you, our valued customer.

What Happened
In late February 2020, we were informed of a possible data security incident affecting our website. We immediately began investigating the potential issue. Our investigation included hiring an outside, expert forensics firm to analyze our systems and determine if there was a breach of our security. On July 20, 2020, that investigation revealed that attackers had succeeded in adding malicious code to our website on July 15, 2019, which allowed unauthorized individuals to capture certain information during the checkout process. We removed that malicious code on July 10, 2020, during an unrelated update of our website ending the unauthorized access to our website.

What Information Was Involved?
On July 20, 2020, we confirmed the possibility that unauthorized individuals may have gained access to your name, shipping and billing address, and the payment card information used to make your purchase on FiltersFast.com.

None of your other personal information was at risk of being impacted during this incident.

What We Are Doing
The security of our customers' information is always a priority, and we sincerely regret any inconvenience to you. We have been working tirelessly to improve the security of our systems to prevent something like this from happening ever again.

Although we think it is unlikely that the unauthorized individuals could use the information collected to steal your identity, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of Credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. Again, we do not believe ID theft to be likely given the data elements involved.

What You Can Do
Please note the following:

- You have zero liability for any purchases that you didn't make.
- Monitor the payment card account used to make your purchase from FiltersFast.com.
- Notify your payment card provider immediately if you notice any suspicious activity.
- Be wary of telephone or email scams.

Please contact ID Experts with any questions or to enroll in free MyIDCare services by calling 833-573-0857 or visiting https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided on the fourth page of this letter. MyIDCare experts are available Monday through Friday from 5 am–5 pm Pacific Time. Please note the deadline to enroll is November 14, 2020.

For More Information

You will find detailed instructions for enrollment on the enclosed Optional Steps. You will need to reference the enrollment code on the fourth page of this letter when calling or enrolling online, so do not discard this letter. Please call 833-573-0857 or visit https://app.myidcare.com/account-creation/protect for assistance or for any additional questions you may have.

Please know that no email from us will request personal information from you. If you receive an email that appears to be from Filters Fast that requests personal information, please do not reply to that email; it is likely to be a scam.

We appreciate your patience and relationship with FiltersFast.com; we understand that this incident is upsetting and sincerely regret that it occurred.

Ray Scardigno
Filters Fast LLC CEO, Founder

MyIDCare

Optional Steps to Help Protect your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state's Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16.

4. Questions and MyIDCare Enrollment. Contact MyIDCare at 833-573-0857 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity. To enroll visit: https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using this Enrollment Code:

To Enroll, Please Call:
833-573-0857
Or Visit: https://app.myidcare.com/account-creation/protect
Enrollment Code: [redacted]9TMC

5. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

New York Residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

FILTERSFAST.COM
Filter. Purify. Protect.

C/O ID Experts
P.O. Box 6336
Portland, OR 97228-6336

0954 [redacted]0875

SANGER POWERS
609 MCGUFFEY DR
MADISON WI 53717-2136

August 18, 2020

Notice of Data Breach

Dear Sanger Powers,

At FiltersFast.com, we are dedicated to our motto to "Filter. Purify. Protect." Since our start in 2004, transparency has been a cornerstone of that commitment. It is in that spirit of transparency that I write to notify you of an incident that may have impacted you, our valued customer.

What Happened
In late February 2020, we were informed of a possible data security incident affecting our website. We immediately began investigating the potential issue. Our investigation included hiring an outside, expert forensics firm to analyze our systems and determine if there was a breach of our security. On July 20, 2020, that investigation revealed that attackers had succeeded in adding malicious code to our website on July 15, 2019, which allowed unauthorized individuals to capture certain information during the checkout process. We removed that malicious code on July 10, 2020, during an unrelated update of our website ending the unauthorized access to our website.

What Information Was Involved?
On July 20, 2020, we confirmed the possibility that unauthorized individuals may have gained access to your name, shipping and billing address, and the payment card information used to make your purchase on FiltersFast.com.

None of your other personal information was at risk of being impacted during this incident.

What We Are Doing
The security of our customers' information is always a priority, and we sincerely regret any inconvenience to you. We ~~have been working tirelessly to improve the security of our systems to prevent something like this from happening~~ ever again.

Although we think it is unlikely that the unauthorized individuals could use the information collected to steal your identity, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of Credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised. Again, we do not believe ID theft to be likely given the data elements involved.

What You Can Do
Please note the following:

- You have zero liability for any purchases that you didn't make.
- Monitor the payment card account used to make your purchase from FiltersFast.com.
- Notify your payment card provider immediately if you notice any suspicious activity.
- Be wary of telephone or email scams.

Please contact ID Experts with any questions or to enroll in free MyIDCare services by calling 833-573-0857 or visiting https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided on the fourth page of this letter. MyIDCare experts are available Monday through Friday from 5 am–5 pm Pacific Time. Please note the deadline to enroll is November 14, 2020.

For More Information
You will find detailed instructions for enrollment on the enclosed Optional Steps. You will need to reference the enrollment code on the fourth page of this letter when calling or enrolling online, so do not discard this letter. Please call 833-573-0857 or visit https://app.myidcare.com/account-creation/protect for assistance or for any additional questions you may have.

Please know that no email from us will request personal information from you. If you receive an email that appears to be from Filters Fast that requests personal information, please do not reply to that email; it is likely to be a scam.

We appreciate your patience and relationship with FiltersFast.com; we understand that this incident is upsetting and sincerely regret that it occurred.

Ray Scardigno
Filters Fast LLC CEO, Founder

MyIDCare

Optional Steps to Help Protect your Information

1. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to your state's Attorney General.

2. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting 1-866-349-5191 P.O. Box 105069 Atlanta, GA 30348-5069 www.equifax.com	Experian Fraud Reporting 1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	TransUnion Fraud Reporting 1-800-680-7289 P.O. Box 2000 Chester, PA 19022-2000 www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

3. Security Freeze. You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; (5) Proof of current address, such as current utility or telephone bill, bank or insurance statement; (6) legible photocopy of government-issued identification card (state driver's license or ID card, military identification, etc.); and (7) if you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. It is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16.

4. Questions and MyIDCare Enrollment. Contact MyIDCare at 833-573-0857 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity. To enroll visit: https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using this Enrollment Code:

To Enroll, Please Call:
833-573-0857
Or Visit: https://app.myidcare.com/account-creation/protect
Enrollment Code: [redacted]WGPV

Enrolled A
8-28-2020
@ 11:15 AM

5. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

6. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580.

New York Residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue NW, Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

JS 44 (Rev. 10/20)

CIVIL COVER SHEET

The JS 44 civil cover sheet and the information contained herein neither replace nor supplement the filing and service of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. *(SEE INSTRUCTIONS ON NEXT PAGE OF THIS FORM.)*

I. (a) PLAINTIFFS

SANGER POWERS & ROBERT LEGG, individually and on behalf of all others similarly situated,

(b) County of Residence of First Listed Plaintiff Dane County, WI
(EXCEPT IN U.S. PLAINTIFF CASES)

(c) Attorneys *(Firm Name, Address, and Telephone Number)*
Shpetim Ademi, Ademi LLP, 3620 East Layton Avenue
Cudahy, WI 53110 (414) 482-8000

DEFENDANTS

FILTERS FAST, LLC

County of Residence of First Listed Defendant _____
(IN U.S. PLAINTIFF CASES ONLY)

NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED.

Attorneys *(If Known)*

II. BASIS OF JURISDICTION *(Place an "X" in One Box Only)*

- ☐ 1 U.S. Government Plaintiff
- ☐ 3 Federal Question *(U.S. Government Not a Party)*
- ☐ 2 U.S. Government Defendant
- ☒ 4 Diversity *(Indicate Citizenship of Parties in Item III)*

III. CITIZENSHIP OF PRINCIPAL PARTIES *(Place an "X" in One Box for Plaintiff and One Box for Defendant)*
(For Diversity Cases Only)

	PTF	DEF		PTF	DEF
Citizen of This State	☒ 1	☐ 1	Incorporated *or* Principal Place of Business In This State	☐ 4	☐ 4
Citizen of Another State	☐ 2	☐ 2	Incorporated *and* Principal Place of Business In Another State	☐ 5	☒ 5
Citizen or Subject of a Foreign Country	☐ 3	☐ 3	Foreign Nation	☐ 6	☐ 6

IV. NATURE OF SUIT *(Place an "X" in One Box Only)*

Click here for: Nature of Suit Code Descriptions.

CONTRACT
- ☐ 110 Insurance
- ☐ 120 Marine
- ☐ 130 Miller Act
- ☐ 140 Negotiable Instrument
- ☐ 150 Recovery of Overpayment & Enforcement of Judgment
- ☐ 151 Medicare Act
- ☐ 152 Recovery of Defaulted Student Loans (Excludes Veterans)
- ☐ 153 Recovery of Overpayment of Veteran's Benefits
- ☐ 160 Stockholders' Suits
- ☒ 190 Other Contract
- ☐ 195 Contract Product Liability
- ☐ 196 Franchise

REAL PROPERTY
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

TORTS

PERSONAL INJURY
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers' Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Personal Injury - Medical Malpractice

PERSONAL INJURY
- ☐ 365 Personal Injury - Product Liability
- ☐ 367 Health Care/ Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Personal Injury Product Liability

PERSONAL PROPERTY
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

CIVIL RIGHTS
- ☐ 440 Other Civil Rights
- ☐ 441 Voting
- ☐ 442 Employment
- ☐ 443 Housing/ Accommodations
- ☐ 445 Amer. w/Disabilities - Employment
- ☐ 446 Amer. w/Disabilities - Other
- ☐ 448 Education

PRISONER PETITIONS

Habeas Corpus:
- ☐ 463 Alien Detainee
- ☐ 510 Motions to Vacate Sentence
- ☐ 530 General
- ☐ 535 Death Penalty

Other:
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Condition
- ☐ 560 Civil Detainee - Conditions of Confinement

FORFEITURE/PENALTY
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

LABOR
- ☐ 710 Fair Labor Standards Act
- ☐ 720 Labor/Management Relations
- ☐ 740 Railway Labor Act
- ☐ 751 Family and Medical Leave Act
- ☐ 790 Other Labor Litigation
- ☐ 791 Employee Retirement Income Security Act

IMMIGRATION
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions

BANKRUPTCY
- ☐ 422 Appeal 28 USC 158
- ☐ 423 Withdrawal 28 USC 157

PROPERTY RIGHTS
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent - Abbreviated New Drug Application
- ☐ 840 Trademark
- ☐ 880 Defend Trade Secrets Act of 2016

SOCIAL SECURITY
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

FEDERAL TAX SUITS
- ☐ 870 Taxes (U.S. Plaintiff or Defendant)
- ☐ 871 IRS—Third Party 26 USC 7609

OTHER STATUTES
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 410 Antitrust
- ☐ 430 Banks and Banking
- ☐ 450 Commerce
- ☐ 460 Deportation
- ☐ 470 Racketeer Influenced and Corrupt Organizations
- ☐ 480 Consumer Credit (15 USC 1681 or 1692)
- ☐ 485 Telephone Consumer Protection Act
- ☐ 490 Cable/Sat TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 890 Other Statutory Actions
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 895 Freedom of Information Act
- ☐ 896 Arbitration
- ☐ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes

V. ORIGIN *(Place an "X" in One Box Only)*

☒ 1 Original Proceeding ☐ 2 Removed from State Court ☐ 3 Remanded from Appellate Court ☐ 4 Reinstated or Reopened ☐ 5 Transferred from Another District *(specify)* ☐ 6 Multidistrict Litigation - Transfer ☐ 8 Multidistrict Litigation - Direct File

VI. CAUSE OF ACTION

Cite the U.S. Civil Statute under which you are filing ***(Do not cite jurisdictional statutes unless diversity)***:
28 U.S.C. § 1332

Brief description of cause:
Negligence, negligence per se, breach of implied contract, unjust enrichment, and violations of consumer protection statutes

VII. REQUESTED IN COMPLAINT:

☒ CHECK IF THIS IS A **CLASS ACTION** UNDER RULE 23, F.R.Cv.P.

DEMAND $

CHECK YES only if demanded in complaint:

JURY DEMAND: ☒ Yes ☐ No

VIII. RELATED CASE(S) IF ANY

(See instructions): JUDGE _____ DOCKET NUMBER _____

DATE
October 26, 2020

SIGNATURE OF ATTORNEY OF RECORD
John D. Blythin

Digitally signed by John D. Blythin
DN: cn=John D. Blythin, o=Ademi LLP, ou, email=jblythin@ademilaw.com, c=US
Date: 2020.10.26 19:55:29 -05'00'

FOR OFFICE USE ONLY

RECEIPT # _____ AMOUNT _____ APPLYING IFP _____ JUDGE _____ MAG. JUDGE _____

INSTRUCTIONS FOR ATTORNEYS COMPLETING CIVIL COVER SHEET FORM JS 44

Authority For Civil Cover Sheet

The JS 44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and service of pleading or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. The attorney filing a case should complete the form as follows:

I.(a) Plaintiffs-Defendants. Enter names (last, first, middle initial) of plaintiff and defendant. If the plaintiff or defendant is a government agency, use only the full name or standard abbreviations. If the plaintiff or defendant is an official within a government agency, identify first the agency and then the official, giving both name and title.

(b) County of Residence. For each civil case filed, except U.S. plaintiff cases, enter the name of the county where the first listed plaintiff resides at the time of filing. In U.S. plaintiff cases, enter the name of the county in which the first listed defendant resides at the time of filing. (NOTE: In land condemnation cases, the county of residence of the "defendant" is the location of the tract of land involved.)

(c) Attorneys. Enter the firm name, address, telephone number, and attorney of record. If there are several attorneys, list them on an attachment, noting in this section "(see attachment)".

II. Jurisdiction. The basis of jurisdiction is set forth under Rule 8(a), F.R.Cv.P., which requires that jurisdictions be shown in pleadings. Place an "X" in one of the boxes. If there is more than one basis of jurisdiction, precedence is given in the order shown below.
United States plaintiff. (1) Jurisdiction based on 28 U.S.C. 1345 and 1348. Suits by agencies and officers of the United States are included here.
United States defendant. (2) When the plaintiff is suing the United States, its officers or agencies, place an "X" in this box.
Federal question. (3) This refers to suits under 28 U.S.C. 1331, where jurisdiction arises under the Constitution of the United States, an amendment to the Constitution, an act of Congress or a treaty of the United States. In cases where the U.S. is a party, the U.S. plaintiff or defendant code takes precedence, and box 1 or 2 should be marked.
Diversity of citizenship. (4) This refers to suits under 28 U.S.C. 1332, where parties are citizens of different states. When Box 4 is checked, the citizenship of the different parties must be checked. (See Section III below**; NOTE: federal question actions take precedence over diversity cases.**)

III. Residence (citizenship) of Principal Parties. This section of the JS 44 is to be completed if diversity of citizenship was indicated above. Mark this section for each principal party.

IV. Nature of Suit. Place an "X" in the appropriate box. If there are multiple nature of suit codes associated with the case, pick the nature of suit code that is most applicable. Click here for: Nature of Suit Code Descriptions.

V. Origin. Place an "X" in one of the seven boxes.
Original Proceedings. (1) Cases which originate in the United States district courts.
Removed from State Court. (2) Proceedings initiated in state courts may be removed to the district courts under Title 28 U.S.C., Section 1441.
Remanded from Appellate Court. (3) Check this box for cases remanded to the district court for further action. Use the date of remand as the filing date.
Reinstated or Reopened. (4) Check this box for cases reinstated or reopened in the district court. Use the reopening date as the filing date.
Transferred from Another District. (5) For cases transferred under Title 28 U.S.C. Section 1404(a). Do not use this for within district transfers or multidistrict litigation transfers.
Multidistrict Litigation – Transfer. (6) Check this box when a multidistrict case is transferred into the district under authority of Title 28 U.S.C. Section 1407.
Multidistrict Litigation – Direct File. (8) Check this box when a multidistrict case is filed in the same district as the Master MDL docket.
PLEASE NOTE THAT THERE IS NOT AN ORIGIN CODE 7. Origin Code 7 was used for historical records and is no longer relevant due to changes in statue.

VI. Cause of Action. Report the civil statute directly related to the cause of action and give a brief description of the cause. **Do not cite jurisdictional statutes unless diversity.** Example: U.S. Civil Statute: 47 USC 553 Brief Description: Unauthorized reception of cable service.

VII. Requested in Complaint. Class Action. Place an "X" in this box if you are filing a class action under Rule 23, F.R.Cv.P.
Demand. In this space enter the actual dollar amount being demanded or indicate other demand, such as a preliminary injunction.
Jury Demand. Check the appropriate box to indicate whether or not a jury is being demanded.

VIII. Related Cases. This section of the JS 44 is used to reference related pending cases, if any. If there are related pending cases, insert the docket numbers and the corresponding judge names for such cases.

Date and Attorney Signature. Date and sign the civil cover sheet.

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

Western District of Wisconsin

SANGER POWERS and ROBERT LEGG, individually and on behalf of all others similarly situated,

Plaintiff(s)

v.

FILTERS FAST, LLC, a North Carolina corporation,

Defendant(s)

Civil Action No. 20-cv-982

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)* Filters Fast, LLC
c/o Ray Scardigno, Registered Agent
5905 Stockbridge Dr.
Monroe, NC 58110-8106

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are: Shpetim Ademi
Ademi LLP
3620 East Layton Avenue
Cudahy, Wisconsin 53110

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No. 20-cv-982

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____ was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____ , a person of suitable age and discretion who resides there, on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is designated by law to accept service of process on behalf of *(name of organization)* _____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____
Server's signature

_____
Printed name and title

_____
Server's address

Additional information regarding attempted service, etc:

Print Save As... Reset