

ATTORNEY GENERAL OF THE STATE OF NEW YORK
BUREAU OF INTERNET & TECHNOLOGY

In the Matter of

Assurance No. 21-015

**Investigation by LETITIA JAMES,
Attorney General of the State of New York, of**

FILTERS FAST LLC,

Respondent.

ASSURANCE OF DISCONTINUANCE

The Office of the Attorney General of the State of New York (“NYAG”) commenced an investigation pursuant to, *inter alia*, Executive Law § 63(12) and General Business Law (“GBL”) §§ 899-aa and-bb into a data security incident at Filters Fast LLC (“Filters Fast” or “Respondent”). This Assurance of Discontinuance (“Assurance”) contains the findings of NYAG’s investigation and the relief agreed to by NYAG and Filters Fast.

NYAG FINDINGS

1. On July 15, 2019, Filters Fast experienced an unauthorized intrusion through a SQL injection attack, where an unknown attacker(s) (the “attacker”) exploited a known vulnerability in a plugin for vBulletin on Filters Fast’s web forum.

2. The attacker targeted Filters Fast’s online checkout process and collected cardholder names, billing addresses, expiration dates, validation codes, and primary account numbers for purchases made on the site between July 16, 2019, and July 10, 2020. In total, approximately 324,000 U.S. residents were affected by the breach, including 16,618 New York

residents.

3. On February 25, 2020, Filters Fast received a Common Point of Purchase (“CPP”) notification from CyberSource, a credit card payment system management company, informing Filters Fast that Discover believed Filters Fast was a common point of purchase for unauthorized purchases occurring on customer credit cards. These reports are usually received by merchants who have an ongoing compromise.

4. In response to the CPP, Filters Fast’s CEO and Senior Web Developer conducted an internal investigation but concluded there was “no evidence of compromised systems.”

5. On March 4, 2020, at Filters Fast’s direction, its hosting provider Flexential rebuilt the company’s webserver out of an abundance of caution. However, as the code introduced into the checkout process remained on the system, the vulnerability remained.

6. On May 13, 2020, MasterCard requested that Filters Fast engage the services of a PCI Forensic Investigator (“PFI”) and conduct an audit of its computer systems, because of additional reports of compromise. Two days later Filters Fast hired Foregenix which began investigating the breach.

7. On May 21, 2020, Foregenix issued its first evaluation of the Filters Fast website environment (titled the “PFI Preliminary Incident Response Report”) that determined there was “no evidence of a breach.” The report stated that “Foregenix has not identified evidence of a breach nor found any malware running on the site at this point in the investigation.” However, in late July, Foregenix reported that it discovered conclusive evidence of a breach. Foregenix reported that the vulnerability exploited by the attacker was rated as “critical” by the National Institute of Standards and Technology and a software patch had been issued to fix it three years

before the company was attacked.

8. Beginning on August 14, 2020, Filters Fast notified affected customers whose credit card information had been affected by the breach.

9. Based on the foregoing, Fast Filters violated Executive Law § 63(12), and GBL §§ 899-aa and -bb.

10. Respondent neither admits nor denies NYAG's Findings, paragraphs 1-9 above.

11. The NYAG finds the relief and agreements contained in this Assurance appropriate and in the public interest. THEREFORE, the NYAG is willing to accept this Assurance pursuant to Executive Law § 63(15), in lieu of commencing a statutory proceeding for violations of Executive Law § 63(12) and GBL §§ 899-aa and -bb.

IT IS HEREBY UNDERSTOOD AND AGREED, by and between the Parties:

PROSPECTIVE RELIEF

12. For the purposes of this Assurance, the following definitions shall apply:

- A. "Customer" shall mean any individual who resides in New York who initiates a purchase of or purchases goods or services from Filters Fast or any individual who resides in New York who otherwise provides Private Information to Filters Fast in connection with an authorized transaction on Filters Fast's website.
- B. "Effective Date" shall be the date of the last signature to this agreement.
- C. "Private Information" shall have the same meaning as private information defined in GBL § 899-aa.

- D. “Security Event” shall mean any compromise that results in unauthorized access to or acquisition of Private Information owned, licensed, or maintained by Filters Fast.

GENERAL COMPLIANCE

13. Filters Fast shall comply with Executive Law § 63(12), and GBL §§ 899-aa and -bb, in connection with its collection, use, and maintenance of Private Information, and shall maintain reasonable security policies and procedures designed to safeguard Private Information from unauthorized use or disclosure.

14. Filters Fast shall not misrepresent the extent to which Filters Fast maintains and protects the privacy, security, confidentiality, or integrity of Private Information collected from or about customers.

INFORMATION SECURITY PROGRAM

15. Filters Fast shall develop, implement, and maintain a written information security program (“Information Security Program”) that is reasonably designed to protect the security, integrity, and confidentiality of Private Information that Filters Fast collects, stores, transmits, and/or maintains. The Information Security Program shall, at a minimum, include the information security requirements set forth in this Assurance.

16. The Information Security Program shall comply with applicable requirements under New York state law, including General Business Law §§ 899-aa and -bb, and shall contain reasonable administrative, technical, and physical safeguards appropriate to: (i) the size and complexity of Filters Fast’s operations; (ii) the nature and scope of Filters Fast’s activities; and (iii) the sensitivity of the Private Information that Filters Fast collects, stores, transmits, and/or

maintains.

17. Filters Fast shall review the Information Security Program not less than annually and make any reasonable changes necessary to ensure the protection of the security, integrity, and confidentiality of Private Information that Filters Fast collects, stores, transmits, and/or maintains.

18. Filters Fast shall appoint a qualified employee to be responsible for implementing, maintaining, and monitoring the Information Security Program with the credentials, background, and expertise in information security appropriate to the level, size, and complexity of her/his role in implementing, maintaining, and monitoring the Information Security Program. Such qualifications may be met by those skills associated with the Payment Card Industry's Security Standards Council's Internal Security Assessor ("ISA") designation. The appointed individual shall report regularly to the Chief Executive Officer concerning Filters Fast's security posture, the security risks faced by Filters Fast, and the Information Security Program.

19. Filters Fast shall provide notice of the requirements of this Assurance to its management-level employees responsible for implementing, maintaining, or monitoring the Information Security Program, and shall implement training of such employees on the requirements of the Private Information Protection Acts and the Security Breach Notification Acts. Filters Fast shall provide the training required under this paragraph to such employees within thirty (30) days of the Effective Date of this Assurance or prior to their responsibilities for implementing, maintaining, or monitoring the Information Security Program.

INCIDENT RESPONSE AND DATA BREACH NOTIFICATION PLAN

20. Within sixty (60) days of the Effective Date of this Assurance, Filters Fast shall develop, implement, and maintain a written incident response and data breach notification plan.

The plan shall identify and describe the following phases: (i) Preparation; (ii) Detection and Analysis; (iii) Containment; (iv) Eradication; and (v) Recovery.

21. The plan shall require that Filters Fast investigate data security incidents that are reasonably suspected to be a Security Event. Filters Fast shall maintain documentation sufficient to show the investigative and responsive actions taken in connection with a Security Event and the determination as to whether notification is required. Filters Fast shall also assess whether there are reasonably feasible training or technical measures, in addition to those already in place, that would materially decrease the risk of the same type of Security Event reoccurring.

22. If Filters Fast determines that a Security Event does not require reporting under the New York state law, Filters Fast shall create a report that includes a description of the Security Event and Filters Fast's response to that Security Event ("Security Event Report"). Filters Fast shall make the Security Event Report available to the NYAG upon request.

PRIVATE INFORMATION SAFEGUARDS AND CONTROLS

23. Encryption: Filters Fast shall encrypt customer Private Information that it collects, stores, transmits and/or maintains, whether stored within the Filters Fast computer network, or transmitted electronically within or outside the network, using a reasonable encryption algorithm.

24. Segmentation: Filters Fast shall segment stored Private Information from any internet-facing application or portal, using a system designed to make Private Information inaccessible from such internet-facing application or portal. If Private Information must be accessible from an internet-facing application or portal for a legitimate and necessary business function, Filters Fast shall employ tokenization in a reasonable manner to minimize any reasonably associated risk.

25. Penetration Testing: Filters Fast shall develop, implement, and maintain a penetration testing program designed to identify, assess, and remediate security vulnerabilities within the Filters Fast computer network. This program shall include regular penetration testing, risk-based vulnerability ratings, and vulnerability remediation practices that are consistent with industry standards.

26. Logging and Monitoring: Filters Fast shall implement and maintain an appropriate system designed to collect and monitor network activity, such as through the use of security and event management tools, as well as appropriate policies and procedures designed to properly configure such tools to report anomalous activity. Logs for network activity should be actively accessible for a period of at least 90 days and stored for at least one year from the date the activity was logged.

27. Anti-Virus Policy: Filters Fast shall implement and maintain a reasonable policy and supporting procedures concerning anti-virus protections. This policy shall be evaluated on an annual basis for ensuring its adequacy and relevancy regarding Filters Fast's needs and goals.

28. Custom Application Code Change Reviews: Filters Fast shall implement and maintain a reasonable policy and supporting procedures concerning custom application code change reviews. This policy will be evaluated on an annual basis for ensuring its adequacy and relevancy regarding Filters Fast's needs and goals.

29. Authentication Policy and Procedures: Filters Fast shall implement and maintain a reasonable policy and supporting procedures implementing industry standard practices for account management and authentication, including forbidding the use of shared user accounts, requiring passwords to be changed at least every 90 days, and requiring the use of multi-factor authentication

to access sensitive systems. It shall be evaluated on an annual basis for ensuring its adequacy and relevancy regarding Filters Fast's needs and goals.

30. Management of Service Providers: Filters Fast shall establish a reasonable policy concerning management of service providers. This policy shall require Filters Fast to clearly define what responsibilities its service providers have with regards to the security of Filters Fast's cardholder data environment, if any. This policy shall be evaluated on an annual basis for ensuring its adequacy and relevancy regarding Filters Fast's needs and goals.

31. Patch Management: Filters Fast shall implement and maintain a reasonable policy to update and patch software on its computer network including the following:

- a. monitoring software and application security updates and security patch management, including but not limited to, receiving notifications from software manufacturers and ensuring the appropriate and timely application of all security updates and/or security patches;
- b. supervising, evaluating, and coordinating any system patch management tool(s); and
- c. training requirement for individuals responsible for implementing and maintaining Fast Filters patch management policies.

INFORMATION SECURITY PROGRAM ASSESSMENTS

32. Within one (1) year of the Effective Date and biennially for five (5) years thereafter, Filters Fast shall obtain assessments of its information security practices by a Payment Card Industry Security Standards Council Qualified Security Assessor ("QSA"). The assessments shall be performed by a QSA with at least three (3) years of experience within the QSA program. The

assessments shall comply with the then current PCI data security standard requirements for reviews by QSAs.

33. Filters Fasts shall pay to the State of New York Two Hundred Thousand Dollars (\$200,000), One Hundred Thousand Dollars (\$100,000) of which shall be suspended. The agreement to suspend One Hundred Thousand Dollars (\$100,000) is expressly premised upon the truthfulness, accuracy, and completeness of Filters Fasts's financial statement submitted to the NYAG. The suspended payment will be immediately due, plus interest computed from the Effective Date, as per the Rules of Court Procedure of the State of New York, if, upon motion, a court finds that Filters Fasts materially misstated its financial condition. The One Hundred Thousand Dollar payment not suspended shall be paid as follows: \$25,000 within seven days after the Effective Date, and \$25,000 on September 30, 2021, December 31, 2021 and March 31, 2022.

MISCELLANEOUS

34. Respondent expressly agrees and acknowledges that NYAG may initiate a subsequent investigation, civil action, or proceeding to enforce this Assurance, for violations of the Assurance, or if the Assurance is voided pursuant to paragraph 41, and agrees and acknowledges that in the event the Assurance is voided pursuant to paragraph 41:

- a. any statute of limitations or other time-related defenses are tolled from and after the Effective Date of this Assurance;
- b. the NYAG may use statements, documents or other materials produced or provided by Respondent prior to or after the Effective Date of this Assurance;

c. any civil action or proceeding must be adjudicated by the courts of the State of New York, and that Respondent irrevocably and unconditionally waives any objection based upon personal jurisdiction, inconvenient forum, or venue; and

d. evidence of a violation of this Assurance shall constitute prima facie proof of a violation of the applicable law pursuant to Executive Law § 63(15).

35. If a court of competent jurisdiction determines that Respondent has violated the Assurance, Respondent shall pay to the NYAG the reasonable cost, if any, of obtaining such determination and of enforcing this Assurance, including without limitation legal fees, expenses, and court costs.

36. This Assurance (including without limitation any and all legal and factual statements herein) is not intended to be and shall not in any event be construed or deemed to be, or represented or caused to be represented as, an admission or concession or evidence of any liability or wrongdoing whatsoever on the part of Filters Fast or of any fact or violation of any law, rule, or regulation. This Assurance is made without trial or adjudication of any alleged issue of fact or law and without any finding of liability of any kind. This Assurance is not intended for use by any third party in any other proceeding.

37. All terms and conditions of this Assurance shall continue in full force and effect on any successor, assignee, or transferee of Respondent. Respondent shall include in any such successor, assignment or transfer agreement a provision that binds the successor, assignee or transferee to the terms of the Assurance. No party may assign, delegate, or otherwise transfer any of its rights or obligations under this Assurance without the prior written consent of NYAG.

38. Nothing contained herein shall be construed as to deprive any person of any private

right under the law.

39. Any failure by the NYAG to insist upon the strict performance by Respondent of any of the provisions of this Assurance shall not be deemed a waiver of any of the provisions hereof, and the NYAG, notwithstanding that failure, shall have the right thereafter to insist upon the strict performance of any and all of the provisions of this Assurance to be performed by Respondent.

40. All notices, reports, requests, and other communications pursuant to this Assurance must reference Assurance No. 21-015, and shall be in writing and shall, unless expressly provided otherwise herein, be given by hand delivery; express courier; or electronic mail at an address designated in writing by the recipient, followed by postage prepaid mail, and shall be addressed as follows:

If to Respondent, to:

Ray Scardigno
Filters Fast LLC
13950 Ballantyne corporate place, Suite 100
Charlotte, NC 28277

If to NYAG, to:

Clark Russell, Deputy Bureau Chief, or in his absence,
to the person holding the title of Bureau Chief
Bureau of Internet & Technology
28 Liberty Street
New York, NY 10005

41. NYAG has agreed to the terms of this Assurance based on, among other things, the representations made to NYAG by Respondent and its counsel and NYAG's own factual investigation as set forth in NYAG's Findings, paragraphs 1-9 above. Respondent represents and warrants that neither it nor its counsel has made any material misrepresentations to NYAG. If any

material misrepresentations by Respondent or its counsel are later found to have been made by NYAG, this Assurance is voidable by NYAG in its sole discretion.

42. No representation, inducement, promise, understanding, condition, or warranty not set forth in this Assurance has been made to or relied upon by Respondent in agreeing to this Assurance.

43. Respondent represents and warrants, through the signature below, that the terms and conditions of this Assurance are duly approved.

44. Except for Paragraphs 13 and 14, the Respondent's obligations under this Assurance shall endure for a period of seven (7) years from the Effective Date. Nothing in this Agreement shall relieve Respondent of other obligations imposed by any applicable state or federal law or regulation or other applicable law.

45. Nothing contained herein shall be construed to limit the remedies available to NYAG in the event that Respondent violates the Assurance after its Effective Date.

46. This Assurance may not be amended except by an instrument in writing signed on behalf of the Parties to this Assurance.

47. In the event that any one or more of the provisions contained in this Assurance shall for any reason be held by a court of competent jurisdiction to be invalid, illegal, or unenforceable in any respect, in the sole discretion of NYAG, such invalidity, illegality, or unenforceability shall not affect any other provision of this Assurance.

48. Respondent acknowledges that it has entered this Assurance freely and voluntarily and upon due deliberation with the advice of counsel.



49. This Assurance shall be governed by the laws of the State of New York without

regard to any conflict of laws principles.

50. The Assurance and all its terms shall be construed as if mutually drafted with no presumption of any type against any party that may be found to have been the drafter.

51. This Assurance may be executed in multiple counterparts by the Parties hereto. All counterparts so executed shall constitute one agreement binding upon all Parties, notwithstanding that all Parties are not signatories to the original or the same counterpart. Each counterpart shall be deemed an original to this Assurance, all of which shall constitute one agreement to be valid as of the Effective Date of this Assurance. For purposes of this Assurance, copies of signatures shall be treated the same as originals. Documents executed, scanned and transmitted electronically and electronic signatures shall be deemed original signatures for purposes of this Assurance and all matters related thereto, with such scanned and electronic signatures having the same legal effect as original signatures.

WHEREFORE, THE SIGNATURES EVIDENCING ASSENT TO THIS Assurance have been affixed hereto on the dates set forth below.

<p>LETITIA JAMES ATTORNEY GENERAL OF THE STATE OF NEW YORK</p> <p>By:  Clark Russell Deputy Bureau Chief Bureau of Internet and Technology New York State Attorney General 28 Liberty St. New York, NY 10005</p> <p><u>5/17/21</u> Date</p>	<p>FILTERS FAST</p> <p>By:  Ray Scardigno, President</p> <p><u>5/17/21</u> Date</p>
---	--