BRYAN CAVE LEIGHTON PAISNER LLP
1155 F Street NW
Washington DC 20004 1357
T: +1 202 508 6000
F: +1 202 508 6200
www.bclplaw.com

August 14, 2020

Joshua James
Direct: 202/508-6265
Fax: 202/508-6200
josh.james@bclplaw.com

Attorney General Tom Miller

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
consumer@ag.iowa.gov

VIA EMAIL

Dear Attorney General Miller:

Filters Fast, LLC ("Filtersfast"), a client of Bryan Cave Leighton Paisner, LLP, is notifying the Office of the Attorney General that Filtersfast is notifying approximtaely 3,272 individuals who reside in Iowa of a criminal cyber-attack on the Filtersfast website. This letter is being provided as a courtesy as we do not believe notification to you is required by your state's statute.

In late February 2020, Filtersfast was made aware of a possible data security incident affecting its e-commerce website. Filtersfast immediately began investigating the potential issue. The investigation included hiring an outside expert forensics firm to analyze the Filtersfast systems and determine if there was a breach of security. On July 20, 2020, that investigation revealed that attackers had succeeded in adding malicious code to the Filtersfast website on July 15, 2019, which allowed unauthorized individuals to capture certain information during the checkout process. The malicious code was removed on July 10, 2020, during an unrelated update of the website, ending the unauthorized access. The information potentially affected includes customer name, shipping and billing address, and payment card information used to make a purchase on the e-commerce site.

Filtersfast is mailing notifications to all potentially affected customers in your state between August 14 and August 18, 2020. An example of the notification is attached. While it is unlikely that this event will result in new account creation identity theft, Filtersfast is offering each potentially affected customer a one-year subscription to identity theft protection services through ID Experts, focused on identifying or remediating existing account fraud that might impact payment card accounts involved. Services include 12 months of credit and CybserScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed ID theft recovery services.

Information regarding these services, as well as additional information to assist customers, is included in the notification sent to the customer.

If you would like additional information concerning the above, please feel free to contact me.

Sincerely,

Joshua James

FILTERSFAST.COM
Filter. Purify. Protect.

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

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice of Data Breach

Dear <<Name 1>>,

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: <<Enrollment Code>>

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.