

October 27, 2023

Via E-Mail: Idtheft@oag.state.md.us

Attorney General Anthony G. Brown
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Re: CommerceV3/Third-Party Data Security Incident

Dear Attorney General Brown:

FisherBroyles, LLP represents Pennsylvania General Store, located at 864 Township Line Rd, Elkins Park, PA 19027, with respect to the data security incident experienced by its third-party vendor, CommerceV3, described in more detail below. Pennsylvania General Store takes the security and privacy of the information seriously and understands CommerceV3 has implemented additional security measures designed to protect the privacy of its customers' data.

1. Description of the Incident.

On or about June 6, 2023, Pennsylvania General Store became aware that its third-party e-commerce platform/vendor, CommerceV3, experienced a data incident which may have impacted the information of certain Pennsylvania General Store customers (the "Incident"). Pennsylvania General Store has since worked diligently to determine what happened and what Pennsylvania General Store information may have been impacted as a result of CommerceV3's Incident. We understand a forensic investigation conducted by CommerceV3 determined that the Incident may have occurred between November 24, 2021 and December 14, 2022.

CommerceV3's investigation, and a subsequent data mining exercise, determined that the name, email address, billing address, payment card number, CVV code and expiration date of certain Pennsylvania General Store customers were potentially accessed and/or acquired by an unauthorized individual.

As of this writing, Pennsylvania General Store has not received any reports of fraud or identity theft related to this matter.

FisherBroyles

2. Number of Maryland residents affected.

Pennsylvania General Store discovered that Incident may have resulted in the unauthorized exposure of information pertaining to three hundred and sixty-one (361) Pennsylvania General Store customers who are residents of Maryland. Notification letters to these individuals were mailed on September 15, 2023, via First Class Mail. A sample copy of the notification letter is attached as **Exhibit A**.

3. Steps taken.

Upon discovery of the Incident, Pennsylvania General Store worked with cybersecurity counsel and CommerceV3 to investigate how the Incident occurred and what Pennsylvania General Store information was potentially impacted by CommerceV3's Incident. In response to the Incident, we understand CommerceV3 has implemented additional security measures designed to protect the privacy of its customers' data.

4. Contact information.

Pennsylvania General Store remains dedicated to protecting the sensitive information within its control and the control of its third-party vendors. If you have any questions or need additional information, please do not hesitate to contact me at Richard.Reiter@fisherbroyles.com or (914) 523-2976.

Very truly yours,

Richard Reiter

Richard Reiter, Partner
FisherBroyles, LLP

Fisher Broyles

EXHIBIT A

The Pennsylvania General Store

Return to IDX:

P.O. Box 989728

West Sacramento, CA 95798-9728



<<First Name>> <<Middle Initial>> <<Last Name>> <<Suffix>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<Zip>>

Via First-Class Mail

September 15, 2023

Notice of Data <<Incident/Breach>>

Dear <<First Name>> <<Middle Initial>> <<Last Name>> <<Suffix>>:

The Pennsylvania General Store was recently alerted to a data security incident that impacted our third-party e-commerce platform, CommerceV3, that may have involved your personal information. Based on our current review, we have no indication that your personal information has been or will be used inappropriately, but we wanted to make you aware of CommerceV3's incident and to provide details on the proactive steps you can take to help protect your information. <<CA Residents: This notification was not delayed by law enforcement.>>

Why Does CommerceV3 Have my Information?

CommerceV3 provides the e-commerce platform we use to process payment card information when an order is placed on our website.

What Happened

While CommerceV3 did not alert the Pennsylvania General Store until June 6, 2023, that data related to its customers may have been impacted, we understand based upon the results of CommerceV3's third-party forensic investigation it was determined the incident occurred between November 24, 2021 and December 14, 2022.

Immediately upon discovering the incident, CommerceV3 conducted a forensic investigation alongside third-party cybersecurity experts as well as the major card brands and banks to assess whether any cardholder data was potentially impacted. CommerceV3 also conducted a review of the potentially affected data to identify the individuals whose information was potentially contained therein for notification purposes. Unfortunately, these types of incidents are becoming increasingly common and even organizations with some of the most sophisticated IT infrastructure available are affected. <<RI Residents: We understand CommerceV3's forensic investigation further determined that the incident potentially impacted approximately forty-six (46) Rhode Island residents who made purchases via the Pennsylvania General Store's online storefront.>>

What Information Was Involved

The elements of your personal information that may have been impacted may have included, and potentially were not limited to, your name, email address, billing address, payment card number, CVV code and expiration date. Please note that we have no evidence at this time that any of your personal information has been misused as a result of the incident.

The Pennsylvania General Store | 864 Township Line Rd, Elkins Park, PA 19027

What We Are Doing

In response to the incident, we understand CommerceV3 has implemented additional security measures designed to protect the privacy of its customers' data.

What You Can Do

At this time, we are not aware of anyone experiencing fraud as a result of CommerceV3's incident. As data incidents are increasingly common, we encourage you to always remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. Additionally, we recommend that you review the following page, which contains important additional information about steps you can take to safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information

Please know that the protection of personal information is a top priority, and we understand the inconvenience and concern this incident may cause. If you have any questions, please do not hesitate to call 1-888-997-7437, Monday – Friday, 9 am – 9 pm ET.

Sincerely,

The Pennsylvania General Store

Additional Important Information

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). 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. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

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; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, 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. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
equifax.com/personal/credit-report-services/
1-800-349-9960

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze

P.O. Box 160
Woodlyn, PA 19094
transunion.com/credit-freeze
1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.

Implementing an Identity Protection PIN (IP PIN) with the IRS:

To help protect against a fraudulent tax return being filed under your name, we recommend Implementing an Identity Protection PIN (IP PIN) with the IRS. An IP PIN is a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS. It helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account.

If you don't already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft. If you want to request an IP PIN, please note: you must pass an identity verification process; and Spouses and dependents are eligible for an IP PIN if they can pass the identity verification process. The fastest way to receive an IP PIN is by using the online Get an IP PIN tool found at: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>. If you wish to get an IP PIN and you don't already have an account on [IRS.gov](https://www.irs.gov), you must register to validate your identity.

Some items to consider when obtaining an IP PIN with the IRS:

- An IP PIN is valid for one calendar year.

- A new IP PIN is generated each year for your account.

- Logging back into the Get an IP PIN tool, will display your current IP PIN.

- An IP PIN must be used when filing any federal tax returns during the year including prior year returns.

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Vermont: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of New Mexico: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfr_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For Residents of Washington, D.C.: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.