

Potomac LAW GROUP

Potomac Law Group, PLLC

William A. McGrath

202.441.6272 | wmcgrath@potomacclaw.com

1717 Pennsylvania Avenue N.W., Suite 1025 | Washington, D.C. 20006

Fax: 202.318.7707

November 27, 2024

VIA EMAIL TO: idtheft@oag.state.md.us

Office of the Attorney General

Attn: Security Breach Notification

200 St. Paul Place

Baltimore, MD 21202

Re: Notification of Security Incident

Dear Madam or Sir,

As legal counsel to STC Holdings LLC, 600 Perdue Avenue, Richmond, VA 23224 (“STC”), we are writing to inform you of a cyber security incident that compromised personal information being entered by customers onto STC’s ecommerce website, TobaccoPipes.com.

1. Nature of the Breach

On November 8, 2024, STC’s ecommerce platform provider (“BigCommerce”) notified STC that a third-party application (“FreshClick”) offered by BigCommerce and used in connection with the tobaccopipes.com website had been compromised. Specifically, BigCommerce advised that a malicious actor had used FreshClick’s compromised third-party application to intercept or “skim” credit card or related information being entered by shoppers on our tobaccopipes.com website. Potentially impacted transactions occurred between October 15 and November 7, 2024. In its email dated November 8, 2024, BigCommerce stated:

“the compromise of the FreshClick application allowed for the injection of malicious script onto the client-facing portion of your store” and the “malicious script may have been used to skim credit card or other information from your shoppers. The malicious actor also compromised the API codes. Your store appears to have been compromised.

...Using our internal tools and communication with the partner we verified that the application was compromised and was being used by a malicious actor to potentially scrape cardholder data and exfiltrate merchant API codes.”

2. What Information Was Involved?

The information that may have been compromised includes names, addresses and payment card information.

3. Number of Individuals and Records Affected

The incident has potentially impacted the personal data of 39 individuals who reside in Maryland.

4. Notification of Affected Individuals

Affected individuals are being provided electronic notice in the form attached on or before November 29, 2024.

4. Contact Information

For further information, please contact:

Name: Carlos Ramos

Title: Head of IT Security and Governance (on behalf of STC)

Email: CarlosR@bethss.com

Telephone: 484-767-6483

with a copy to: stcdatabreach@potomacclaw.com

5. Measures Taken

To address and mitigate the impact of the incident, the following measures have been, or are being, undertaken:

- BigCommerce uninstalled the FreshClick app from STC’s ecommerce website immediately upon learning of the Incident. BigCommerce also removed compromised API’s and malicious code, if any, from STC’s website.
- STC’s IT team secured its systems to prevent any unauthorized access.
- STC’s IT team is engaging with outside experts to conduct an independent forensics investigation into the matter to determine any necessary remedial measures.
- STC is notifying all potentially affected customers.

November 27, 2024
Page 3 of 3

STC is committed to taking all necessary steps to address this incident. Please don't hesitate to contact us with any questions.

Sincerely,

William A. McGrath

William A. McGrath
Counsel for STC HOLDINGS LLC

CC: STC Holdings LLC

November **XX**, 2024

Subject: Notice of Data Security Incident

Dear Customer:

We are writing to notify you of a data security incident that may have resulted in unauthorized access to some of the personal information you submitted while visiting the tobaccopipes.com website. As part of our ongoing commitment to transparency and privacy, we are writing to explain the details of this breach, the actions we are taking to resolve it, and the steps you can take to protect yourself.

What Happened?

On November 8, 2024, our ecommerce platform provider (“BigCommerce”) notified us that a third-party application (“FreshClick”) offered by BigCommerce and used in connection with the tobaccopipes.com website had been compromised. Specifically, BigCommerce advised that a malicious actor had used FreshClick’s compromised third-party application to intercept or “skim” credit card or related information as it was being entered by shoppers on our tobaccopipes.com website. Potentially impacted transactions occurred between October 15 and November 7, 2024.

What Information Was Involved?

The information that may have been compromised includes names, addresses, and credit card information.

What We Are Doing

Since learning about this incident, we and our partners and agents immediately have taken, or are taking, the following steps to remediate and resolve the issue:

1. **Immediately uninstalled the compromised third-party application** from our ecommerce website (www.tobaccopipes.com).
2. **Secured our systems** to prevent further unauthorized access.
3. **Engaging security experts** to conduct an independent forensics investigation.
4. **Notifying relevant government agencies** in accordance with applicable data privacy laws.

5. **Notifying individuals**, like yourself, whose information may have been compromised.

What You Can Do

We take our obligation to safeguard personal information very seriously and are alerting you about this issue so you can take steps to help protect your information:

- **Change your passwords:** Update the passwords for your tobaccopipes.com account and any other online accounts that may use the same credentials.
- **Contact your bank or credit card company to cancel your card and request a new one.**
- **Monitor your credit card accounts:** Review your transactions regularly, including account records and statements, and check for any suspicious activity.
- **Request your free credit report:** You are entitled under U.S. law to one free credit report annually from each of the three major consumer reporting agencies. See Additional Resources below for more useful information.
- **Sign up to receive instant notifications** of potential suspicious activity by enabling notifications or alerts in your accounts.

For More Information

We understand how unsettling this news must be, and we are here to help you through the process. For more details about this issue, please contact our customer care team at 1-800-542-4013 or Customercare@tobaccopipes.com.

We sincerely apologize for any inconvenience this may have caused and appreciate your understanding as we address this matter. We will provide updates if further significant developments arise.

Sincerely,

Terry Williams, President
TobaccoPipes.com

Additional Resources:

- **Visit the Federal Trade Commission (FTC)** website for information on how to protect yourself against ID theft and safeguarding your electronic devices from viruses, hacking and other malicious attacks: consumer.gov/idtheft or call 1-877-IDTHEFT (438-4338) to learn more about identity theft and protective steps you can take or file a report. You can also contact the FTC at: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington DC 20580.
- **Exercise your rights under the federal Fair Credit Reporting Act (FCRA).** The FCRA promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. Under the FCRA, the major consumer reporting companies are required to provide you with a copy of the information in your report if you request it. To order your free annual credit report, visit www.annualcreditreport.com or call toll-free at 1-877-322-8228. Additionally, all consumer reporting companies must provide you with a copy of your information, whenever requested, for a reasonable fee. Further, the consumer reporting agencies must give you a free copy of your information if you request it after an adverse action is taken against you based on information in your report. For more information about the FCRA, including information about your rights, go to consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.
- **Contact the major consumer reporting agencies** to get useful information about protecting your credit, including information about fraud alerts, security freezes, or other steps you can take to protect yourself from fraud and identity theft.
 - **Equifax:** equifax.com equifax.com/credit-freeze/ 1-800-525-6285 P.O. Box 105788, Atlanta, GA 30348
 - **Experian:** experian.com experian.com/help/credit-freeze/ 1-888-397-3742 P.O. Box 9554, Allen, TX 75013
 - **TransUnion:** transunion.com transunion.com/credit-freeze 1-800-680-7289 P.O. Box 160, Woodlyn, PA 19094
- **Review your free credit reports.** When you receive a credit report from each agency, review the reports carefully. Look for accounts you did not open, inquiries from creditors that you did not initiate, and confirm that your personal information, such as home address and Social Security number, is accurate. If you see anything you do not understand or recognize, call the credit reporting agency at the telephone number on the report. If necessary, you should also call your local police department and file a report. Get and keep a copy of the police report because you may need to give copies to creditors to clear up your records or to access transaction records.

- **Consider placing a fraud alert on your credit reports.** A fraud alert conveys a special message to anyone requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you have authorized the request. A fraud alert should not stop you from using your existing credit cards or other accounts, but it may slow down your ability to get new credit. An initial fraud alert is valid for ninety (90) days. To place a fraud alert, contact one of the three major credit reporting agencies. One agency will notify the other two on your behalf. You will then receive letters from the agencies with instructions on how to manage your alerts.
- **Consider placing a free credit freeze on your credit reports.** A credit freeze restricts access to your credit report, which means you — or others — won't be able to open a new credit account while the freeze is in place. You can temporarily lift the credit freeze if you need to apply for new credit. When the freeze is in place, you will still be able to do things like apply for a job, rent an apartment, or buy insurance without lifting or removing it. Your free credit freeze lasts until you remove it. To learn more, contact each of the three consumer reporting agencies — Equifax, Experian, and TransUnion.

For District of Columbia Residents. You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia: Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington, D.C. 20001, (202)-727-3400, www.oag.dc.gov

For Iowa Residents. You may report suspected incidents of identity theft to local law enforcement or the Iowa Attorney General. Iowa Attorney General's Office, 1305 E Walnut St, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov

For Maryland Residents. You can obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: 200 St. Paul Place, Baltimore, MD 21202, (888)743-0023 www.marylandattorneygeneral.gov

For Massachusetts Residents. You have the right to obtain a police report, if any, and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request to place a security freeze on your account.

For North Carolina Residents. You can obtain information from the North Carolina Attorney General's Office about preventing identity theft: North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699-9001, (877) 566-7226 (toll-free in North Carolina), (919) 716-6400, www.ncdoj.gov

For Oregon Residents. You may report suspected incidents of identity theft to law enforcement or the Federal Trade Commission (FTC). The Department of Justice may be contacted as follows: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301, (877) 877-9392, www.doj.state.or.us

For Rhode Island Residents. You can obtain information from the Rhode Island Office of the Attorney General about preventing identity theft: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903 (401) 274-4400 www.riag.ri.gov