ECKERT SEAMANS
ATTORNEYS AT LAW

Eckert Seamans Cherin & Mellott, LLC
U.S. Steel Tower
600 Grant Street, 44th Floor
Pittsburgh, PA 15219

TEL: 412 566 6000
FAX: 412 566 6099

Matthew H. Meade, Esq.
(412) 566-6983
mmeade@eckertseamans.com

March 15, 2022

VIA EMAIL: CONSUMER@AG.IOWA.GOV

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

Re: Supplemental Notice of Data Security Incident

Dear Attorney General Miller:

This notice is provided on behalf of my client, Penn LLC d/b/a PulseTV ("PulseTV") as a supplement to the notice that PulseTV submitted on January 25, 2022 (the "Prior Notice"). The Prior Notice advised that PulseTV experienced a data breach involving PulseTV's website and the credit card information of one thousand two hundred and eighty four (1,284) Iowa residents. Although PulseTV had not confirmed the cause of the data breach when it sent the earlier notices, PulseTV determined that in an abundance of caution, it would provide written notice to these individuals in January of 2022.

On February 2, 2022, PulseTV's continuing investigation revealed that the incident was caused by a malware attack on a webserver hosted and maintained by Freestyle Solutions, a software vendor that hosts PulseTV's website, among others'. The malware captured PulseTV customers' card data and saved it to a file on Freestyle's systems, which PulseTV could not access. PulseTV immediately alerted Freestyle, instructed them to disable the malware, and confirmed that it was successfully disabled. On February 15, 2022, the PCI-DSS Forensic Investigator confirmed to PulseTV that the period of potential compromise ended on February 2, 2022. As a result, PulseTV will be sending a new round of notices to customers whose credit cards could have been compromised between September 1, 2021 and February 2, 2022.

After working with a vendor to locate current addresses for these individuals, PulseTV learned, on February 24, 2022, that the new round of notifications will include two hundred fourteen (214) Iowa residents. A copy of the notice letter that will be mailed to these individuals on March 15, 2022 and March 17, 2022 is enclosed. Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,

/s/ Matthew H. Meade, Esq.

ECKERT SEAMANS
ATTORNEYS AT LAW

MHM/
Enclosure

7851 185th St. • Suite 106 • Tinley Park, IL 60477 Pulsetv.com™

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

IMPORTANT INFORMATION
PLEASE REVIEW CAREFULLY
UPDATE

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

PulseTV is writing to provide an update to the data security notice that you should have received at the beginning of the year. In connection with our ongoing investigation, we recently learned that the incident was caused by a malware attack at Freestyle Solutions, Inc., a software vendor that hosts our website. We also learned that payment card transactions on our website between September 1, 2021 and February 2, 2022 may be at risk. You are receiving this update because you made a purchase during this time frame using a different credit card than the card you used the first time we notified you. We take this matter very seriously because we know how important this information is to you. We are providing this notice to you as a precautionary measure, to inform you of the incident, and to explain steps that you can take to protect your information.

What Happened

As explained in our previous letter, a credit card company notified us in March of 2021 that our website (www.pulsetv.com) was a common point of purchase for some unauthorized credit card transactions. After scanning our systems for malware, checking our security settings, and cooperating with card brand investigations, we did not find any ongoing compromise of customer cards at that time and were unable to verify our website as the cause of the unauthorized transactions. A few months later, we heard from the card brands and law enforcement about additional payment card compromises that appeared to originate from our website. We then started working with legal counsel that specializes in cybersecurity. Legal counsel also hired nationally-recognized digital forensics experts to assist us.

After several weeks of investigation, we had still not confirmed the cause of the unauthorized transactions. However, in an abundance of caution, at the end of December 2021 and early January 2022, we notified those customers, like you, whose credit cards had been used during the timeframes provided by the card brands. After notifying consumers, we continued to work closely with the card brands and multiple cybersecurity firms to determine the source of the unauthorized charges.

On February 2, 2022, our continuing investigation revealed that the incident was caused by a malware attack on a webserver hosted and maintained by Freestyle Solutions, Inc., a software vendor that hosts our website. The malware captured our customers' card data and saved it to a file on Freestyle's systems, which we could not access. We immediately alerted Freestyle, instructed them to disable the malware, and confirmed that it was successfully disabled.

What Information Was Involved

The affected information may have included your name, address, email address, payment card number, expiration date, and card security code (CVV) provided during checkout.

What We Are Doing

When we discovered this incident, we launched an investigation. Although multiple forensic investigators were unable to verify our website as the cause of the unauthorized transactions, we continued to investigate until we found the source of the incident. Once we discovered that the issue originated on Freestyle's systems, we immediately alerted Freestyle and confirmed that they disabled the malware responsible for the incident.

Additionally, because cyber threats are always evolving, we are continuously working to identify and mitigate threats and evaluate our IT security protocols to make sure that sensitive data is protected. In addition, to further improve our website security and help prevent similar occurrences in the future, we have taken, or will be taking, the following steps:

1. Adding two-factor authentication requirements for all internal devices;
2. Utilizing end-point detection and response tools to provide greater network visibility and threat mitigation; and
3. Migrating to a different payment system.

We are continuing to work with the card brands to keep them informed and cooperating with ongoing investigations of the incident by law enforcement. Finally, we are providing notice of this incident to appropriate state regulators, consistent with our compliance obligations and responsibilities.

What You Can Do

We recommend that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. Information on additional ways to protect your information, including how to obtain a free credit report and free security freeze, can be found at the end of this letter. You should report any incidents of suspected identity theft to your local law enforcement and state Attorney General.

If you believe your payment card information may have been compromised, we strongly encourage that you contact your payment card company and/or financial institution and request that the card be cancelled.

For More Information

Please accept our apologies that this incident occurred. You are a valued customer and appreciate that you came back to us with your business. The privacy and security of your information is very important to us and we remain committed to maintaining the confidentiality of your information. **If you have any further questions, please contact us at 1-855-618-3212, Monday through Friday, 9:00 a.m. to 6:30 p.m., Eastern Time (excluding some U.S. holidays).**

Sincerely,

Tom Zegar,
Co-Founder & Vice President
Pulsetv.com

MORE INFORMATION ABOUT IDENTITY THEFT AND WAYS TO PROTECT YOURSELF

Visit www.experian.com/credit-advice/topic-fraud-and-identity-theft.html for general information regarding identity protection. You can obtain additional information about fraud alerts, security freezes, and preventing identity theft from the consumer reporting agencies listed below and the Federal Trade Commission (FTC) by calling its identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information online at www.consumer.ftc.gov/features/feature-0014-identity-theft. The FTC's address is: Federal Trade Commission, Division of Privacy and Identity Protection, 600 Pennsylvania Avenue, NW, Washington, DC 20580. You have the ability to place a security freeze on your credit reports by contacting the following agencies.

National Credit Reporting Agencies Contact Information

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-888-298-0045	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

Obtain Your Credit Report

You should also monitor your credit reports. You may periodically obtain your credit reports from each of the national consumer reporting agencies. In addition, under federal law, you are entitled to one free copy of your credit report every 12 months from each of the three nationwide consumer reporting agencies listed above. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You also may complete the Annual Credit Report Request Form available from the FTC at www.consumer.ftc.gov/articles/pdf-0093-annual-report-request-form.pdf and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also contact any of the three major consumer reporting agencies to request a copy of your credit report.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly.

If you discover inaccurate information or a fraudulent transaction on your credit report, you have the right to request that the consumer reporting agency delete that information from your credit report file.

Fraud Alerts

You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any new accounts in your name. To place a fraud alert on your credit report, contact any of the three national credit reporting agencies using the contact information listed above. As soon as one credit bureau confirms the fraud alert, they will notify the others. Additional information is available at www.annualcreditreport.com.

Security Freeze

You have the ability to place a security freeze on your credit report at no cost to you. 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 may be able to use an online process, an automated telephone line, or a written request to all three of the credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, 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) a legible copy of a government-issued identification card, (6) proof of current address, such as a legible copy of a recent utility bill or bank or insurance statement, (7) a legible copy of a recent W-2, pay stub, or Social Security card, and (8) if you are a victim of identity theft, 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. **Under federal law, you cannot be charged to place, lift, or remove a security freeze.**

After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place, you will need it if you choose to lift the freeze. If you do place a security freeze *prior* to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

Additional Helpful Information

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them at the information provided above.

If this notice letter states that your financial account number and/or credit or debit card number was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account(s), including whether you should close your account(s) or obtain a new account number(s).

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name, or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

STATE SPECIFIC INFORMATION

DISTRICT OF COLUMBIA residents: You may also obtain information about preventing and avoiding identity theft from the D.C. Attorney General's Office. This office can be reached at: Office of the Attorney General of the District of Columbia, Office of Consumer Protection, 441 4th Street, NW, Washington, D.C. 20001 www.oag.dc.gov 1-202-7273400

MARYLAND residents: You may also obtain information about preventing and avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 www.oag.state.md.us/Consumer Toll-free: 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 Ave. N.W., Washington, D.C. 20580.

NEW YORK residents: You may also obtain information on identity theft from the New York Department of State Division of Consumer Protection or the New York Attorney General. These agencies can be reached at:

New York Department of State Division of Consumer Protection	New York Attorney General
1-800-697-1220	1-800-771-7755
http://www.dos.ny.gov/consumerprotection	http://www.ag.ny.gov/home.html

NORTH CAROLINA residents: You may also obtain information about preventing and avoiding identity theft from the North Carolina Attorney General's Office. This office can be reached at: North Carolina Department of Justice, Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699 www.ncdoj.gov Toll-free: 1-877-566-7226 Toll-free: 1-877-566-7226

RHODE ISLAND residents: You have the right to file and obtain a copy of a police report concerning any fraud or identity theft committed using your personal information. You may also obtain information about preventing and avoiding identity theft from the Rhode Island Attorney General's Office. This office can be reached at: Office of the Attorney General, 150 South Main Street, Providence, RI 02903 www.riag.ri.gov Toll-free: 1-401-274-4400