

To Whom It May Concern,

On behalf of our client, Stiiizy, Inc., I am writing to notify the Maryland Office of the Attorney General of a recent security breach.

On November 20, 2024, Stiiizy was notified by its vendor of point-of-sale processing services that accounts with their organization had been compromised by an organized cybercrime group. Personal information of Stiiizy customers processed by the vendor was acquired by the threat actors during that time.

Based on the information currently available to Stiiizy, the incident affected around 1500 Maryland residents' personal information, including drivers' license numbers and other state identification numbers. Stiiizy has engaged legal counsel and cybersecurity consultants to assist in addressing the incident. Additionally, Stiiizy will be providing free credit monitoring services to affected individuals.

A sample copy of the draft notice to be sent out to Maryland consumers is attached.

If there are any questions, please do not hesitate to contact my office.

Best,

Amira Bucklin

18575 Jamboree Road, 9th Floor | Irvine, CA 92612

O. (714) 641-5100 | D. (714) 641-3431

abucklin@rutan.com | www.rutan.com



Privileged And Confidential Communication.

This electronic transmission, and any documents attached hereto, (a) are protected by the Electronic Communications Privacy Act (18 USC §§ 2510-2521), (b) may contain confidential and/or legally privileged information, and (c) are for the sole use of the intended recipient named above. If you have received this electronic message in error, please notify the sender and delete the electronic message. Any disclosure, copying, distribution, or use of the contents of the information received in error is strictly prohibited.

STIIIZY, Inc.

[DATE]

Enrollment Code: [CODE]

[Individual Name]

[Street address]

[City, state, and postal code]

NOTICE OF DATA BREACH

Dear [Individual Name]:

Stiiizy, Inc. (“STIIIZY”) values the trust you place in us and takes the privacy and security of your information very seriously. We are writing to inform you about a data security incident that may involve your personal information processed by one of STIIIZY’s vendors. We have also notified law enforcement of the incident.

What Happened?

On November 20, 2024, we were notified by a vendor of point-of-sale processing services for some of our retail locations that accounts with their organization had been compromised by an organized cybercrime group. An investigation conducted by the vendor revealed that personal information relating to certain STIIIZY customers processed by the vendor was acquired by the threat actors on or around October 10, 2024 - November 10, 2024. Upon receiving notice of the incident, we launched our own investigation to assess the extent of the impact. We have determined that certain of our customers’ personal information and documents was acquired by the threat actors. We have been working closely with the vendor and our legal counsel to address the situation, including to determine the cause of the incident. This notification was not delayed by law enforcement.

What Information Was Involved?

If you are receiving this letter, STIIIZY has determined that you are part of the group of individuals whose personal information was affected by this incident. The impacted records contained personal information contained on government-issued identification cards, including drivers’ licenses and medical cannabis cards, as well as information related to transactions with our dispensaries. Not all of this information was affected for each impacted individual.

What We Are Doing

STIIIZY values your privacy and deeply regrets that this incident occurred. STIIIZY has implemented additional security measures designed to prevent a recurrence of such an attack and to protect the privacy of STIIIZY’s valued customers. Additionally, we are providing affected individuals with free credit monitoring services, as described more fully below.

What You Can Do

STIIIZY encourages you to remain vigilant against incidents of identity theft and fraud, to review account statements, and to monitor credit reports for suspicious or unauthorized activity. Additionally, security experts suggest individuals to contact their financial institution and major credit bureaus to inform them

of such a breach and take whatever steps are recommended to protect your interests, including the possible placement of a fraud alert on credit files.

As a precautionary measure, and to assist you in protecting yourself against identity theft, STIIIZY is providing each potentially impacted individual with a complimentary 12-month membership of [Service]. This product provides you with identity theft detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by:** [Activation Deadline] (Your code will not work after this date.)
- **Visit** the [Service] website to enroll: [URL]
- Provide your **activation code** provided at the top of this notice.

If you have any questions about the product, or need assistance with identity restoration, please contact [Service's] customer care team at [phone number] by [Activation Deadline].

In the meantime, we encourage you to take the following steps to further protect your information:

1. Closely monitor your financial account and promptly contact your financial institution if you notice any unusual activity.
2. Report incidents of suspected identity theft to your local law enforcement, the Federal Trade Commission, and your state attorney general. To file a complaint with the FTC, go to IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies. Information on how to contact your state attorney general may be found at www.naag.org/naag/attorneys-general/whos-my-ag.php.
3. Take advantage of additional free resources on identity theft. We recommend that you review the tips provided by the Federal Trade Commission's Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>.

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC's website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf.

4. Monitor your free credit reports. You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <https://www.annualcreditreport.com>, by calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348.
5. Place a security freeze on your credit files by contacting each of the three credit reporting agencies (Equifax, Experian, and TransUnion). Freezing credit files will prevent someone from using your personal information to open new accounts or borrow money in your name. To place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank

statement, or insurance statement. Please understand that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card unless you temporarily or permanently remove the freeze. There is no charge to request a security freeze or to remove a security freeze.

6. Contact the three credit reporting agencies to notify them of this incident, receive credit alerts, or freeze your credit file. Contact information for the three agencies is provided below:

Equifax	Experian	TransUnion
(866) 349-5191 www.equifax.com P.O. Box 740241 Atlanta, GA 30374	(888) 397-3742 www.experian.com P.O. Box 2002 Allen, TX 75013	(800) 888-4213 www.transunion.com P.O. Box 1000 Chester, PA 19016

For More Information

We understand that this incident may cause concern, and we are committed to providing you with the support you need. If you have questions, please call our dedicated call center at **[CALL CENTER NUMBER AND AVAILABILITY INFO]**.

Thank you for your patience and understanding as we work through this progress.

Sincerely,

[SIGNATURE BLOCK]

ADDITIONAL IMPORTANT INFORMATION

More information can also be obtained by contacting the Federal Trade Commission: Federal Trade Commission - Consumer Response Center: 600 Pennsylvania Ave, NW, Washington, DC 20580; 1-877-IDTHEFT (438-4338); www.identitytheft.gov

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: You are advised to 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 Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach. You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Rhode Island: The Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Individuals have the right to obtain any police report filed in regard to this event. There are approximately 154 Rhode Island residents that may be impacted by this event.

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

District of Columbia Office of the Attorney General – Office of Consumer Protection: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov

Illinois Office of the Attorney General: 100 West Randolph Street, Chicago, IL 60601; 1-866-999-5630; www.illinoisattorneygeneral.gov

Maryland Office of the Attorney General - Consumer Protection Division: 200 St. Paul Place, 16th floor, Baltimore, MD 21202; 1- 888-743-0023; www.oag.state.md.us

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>

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