Notice of Data Security Incident

Philadelphia, Pennsylvania (April 1, 2026) – Weavers Way Cooperative Association ("Weavers Way Co-Op") is committed to protecting the privacy and security of the personal information it maintains. Weavers Way Co-Op is making individuals aware of a data security incident that impacted a limited number of its customers. Weavers Way Co-Op is making potentially affected individuals aware of the incident and steps that impacted individuals can take to protect their personal information.

Recently, Weavers Way Co-Op learned that an unauthorized party placed a skimmer device on the PIN pad of one of the check-out registers within its Mt. Airy store. This skimmer device allowed the unauthorized party to access payment information for a limited number of customers who used the check-out register from on or about January 1, 2026, to on or about March 3, 2026. Upon learning of this issue, Weavers Way Co-Op immediately launched an investigation and coordinated with law enforcement.

Following a comprehensive investigation and manual internal review, on March 6, 2026, Weavers Way Co-Op concluded that some of the transactions accessed and/or acquired by the unauthorized party as a result of this incident contained certain personal information pertaining to particular individuals. The personal information contained within the potentially impacted data credit, debit, or SNAP card numbers with or without access information. The types of impacted information varied by individual.

On April 1, 2026, Weavers Way Co-Op mailed written notification letters to individuals whose information was determined to be involved in this incident, to the extent that valid mailing addresses were available. For individuals who have questions or need additional information regarding this incident, or to determine if they are impacted, Weavers Way Co-Op has established a dedicated toll-free response line at (844) 403-4532. The response line is available between the hours of 9:00 a.m. to 6:30 p.m. Eastern Time, Monday through Friday, excluding holidays.

– OTHER IMPORTANT INFORMATION –

1. Placing a Fraud Alert on Your Credit File.

We recommend that you place an initial one (1) year "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call anyone (1) of the three (3) major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

Experian
P.O. Box 9554
Allen, TX 75013
https://www.experian.com/fraud/center.html
(888) 397-3742

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three (3) nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three (3) credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348-5788
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. 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.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one (1) free credit report every twelve (12) months from each of the above three (3) major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

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 on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600

Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

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

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.

For those who have SNAP benefits, the Pennsylvania Department of Human Services offers a mobile application called "ConnectEBT" that allows you to view your balance, change your PIN, and lock your card when it is not in use. More information on verifying and securing your SNAP benefits can be found at https://www.pa.gov/agencies/dhs/resources/snap/ebt or by calling the EBT Recipient Hotline at **1-888-EBT-PENN** (1-888-328-7366).

* * *