Victron Energy, Inc.
Notice of Data Security Incident

Updated: August 5, 2025

Victron Energy, Inc. ("Victron") is committed to protecting the privacy and security of the personal information we maintain. Victron is making individuals aware of a data security incident that impacted Victron's internal systems. Although we have no evidence of financial fraud or identity theft related to this incident, we are making potentially affected individuals aware of the incident, the resources we are making available to those affected, and steps that impacted individuals can take to best protect their personal information, should they feel it appropriate to do so.

What Happened? Recently, Victron learned that an unauthorized party gained access to a limited number of internal systems on October 5, 2024. Upon detecting the unauthorized activity, Victron immediately contained the incident and launched a thorough investigation. As a part of the investigation, Victron engaged leading outside cybersecurity professionals to secure the environment and to identify the scope of what personal information, if any, was involved.

Following a comprehensive forensic investigation and manual document review exercise, Victron discovered on or about July 24, 2025, that one or more of the files or folders accessed and/or acquired by the unauthorized party as a result of this incident contained certain personal information pertaining to particular individuals.

To date, we have no evidence of financial fraud or identity theft related to this incident. Nevertheless, we will be providing notice of the incident to the individuals whose personal information was potentially impacted.

What Information Was Involved? The impacted data included full names, Social Security numbers, dates of birth, driver's license numbers or other state identification numbers, financial account and routing number information, taxpayer identification numbers, passport numbers, payment card information, medical condition and treatment information, health insurance information, patient identification numbers, medical record numbers, medical diagnosis information, username and passwords, and biometric information. The types of impacted information varied by individual.

What We Are Doing. The security and privacy of the information we maintain is a top priority for us. In response to this incident, we took immediate steps to secure our network environment and engaged third-party forensic experts to assist in the investigation. Victron continually evaluates and modifies its practices and internal controls to enhance the security and privacy of individual personal information and will continue to do so in light of this incident.

How will Individuals Know if They are Affected by this Incident? Victron is providing notice to individuals whose information was determined to be affected by this incident, in accordance with our legal obligations and to the extent we have valid mailing addresses for the individuals. We will also be providing complimentary credit monitoring memberships to individuals whose Social Security numbers have been determined to be impacted. If an individual does not receive a

letter but would like to know if they are potentially affected, they may call the call center we have established to respond to inquiries about this matter at 1-800-939-4170.

For More Information. If you have any questions regarding this incident, please call the dedicated and confidential toll-free response line at 1-800-939-4170. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to protect against potential misuse of your information. The response line is available from Monday through Friday, 8:00 a.m. to 8:00 p.m. Central Time, excluding holidays.

What You Can Do. We encourage individuals to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, explanation of benefits forms, and monitoring your free credit reports for suspicious activity and to detect errors. Under U.S. law individuals are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Individuals may also contact the three major credit bureaus directly to request a free copy of their credit report, place a fraud alert, or a security freeze. Contact information for the credit bureaus is below:

— OTHER IMPORTANT INFORMATION—

1. **Placing a Fraud Alert on Your Credit File.**

You may place an initial one-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 any one of the three 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 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 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.

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.

If you do place a security freeze *prior* to enrolling in any credit monitoring service, if offered to you in your letter, 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.

3. Additional Information

You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

4. Protecting Your Medical Information.

The following practices can provide additional safeguards to protect against medical identity theft.

- Only share your health insurance cards with your health care providers and other family members who are covered under your insurance plan or who help you with your medical care.

- Review your "explanation of benefits statement" which you receive from your health insurance company. Follow up with your insurance company or care provider for any items you do not recognize. If necessary, contact the care provider on the explanation of benefits statement and ask for copies of medical records from the date of the potential access (noted above) to current date.
- Ask your insurance company for a current year-to-date report of all services paid for you as a beneficiary. Follow up with your insurance company or the care provider for any items you do not recognize.

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. In addition, you have the right to obtain a security freeze (as explained above) or submit a declaration of removal. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act. For more information about the FCRA, please visit www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755 (TDD/TYY Support: 800-788-9898); Medicare Fraud Control Unit Direct Line: 212-417-5397.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392.

*** * ***