# Coldcard Security Flaw Raises Risks for Certain Bitcoin Wallets

**Client Advisories**

08.04.2026

By: Brian M. McGovern

---

A recently disclosed security flaw affecting certain Coldcard hardware wallets has been linked to a series of suspected Bitcoin thefts reportedly totaling tens of millions of dollars. Although the scope of the incident remains under investigation, Coinkite—the manufacturer of Coldcard wallets—has recommended that many users migrate affected wallets to newly generated recovery phrases.

The incident serves as an important reminder that storing cryptocurrency offline substantially reduces cybersecurity risk but does not eliminate every risk. Investors, businesses, trustees, executors and other fiduciaries holding Bitcoin should determine whether their assets may be affected and review their digital-asset custody procedures.

**What Happened?**

Coldcard is a popular hardware wallet manufactured by Canadian company Coinkite. Unlike software wallets or cryptocurrency exchanges, a hardware wallet stores the cryptographic credentials needed to control Bitcoin offline, making it one of the most secure methods of custody.

A Bitcoin wallet is controlled through private cryptographic information. When a wallet is created, the owner receives a “seed phrase” or “recovery phrase”—usually 12 or 24 words—that functions as the master key. Anyone who obtains or reconstructs that phrase can transfer the Bitcoin without possessing the physical device.

Security researchers recently discovered that certain versions of Coldcard firmware did not generate recovery phrases with the expected degree of randomness. As a result, the flaw may have made some recovery phrases substantially easier for a sophisticated attacker to predict.

Attackers who reconstructed vulnerable recovery phrases were able to locate the associated Bitcoin addresses on the public blockchain and transfer the funds without having physical access to the Coldcard device.

Blockchain investigators have identified several suspected waves of theft involving Coldcard-generated addresses. Public reports place suspected losses above $80 million, with some estimates exceeding $100 million. The precise amount stolen, the number of affected investors, and the connection between every suspicious transaction and this flaw remain under investigation.

Importantly, the vulnerability relates to the firmware installed when the recovery phrase was originally generated, not necessarily the firmware currently installed on the device.

According to Coinkite, potentially affected wallets include recovery phrases generated using:

- Coldcard Mk2 or Mk3 firmware versions 4.0.1 through 4.1.9
- Coldcard Mk4 or Mk5 firmware predating version 5.6.0
- Coldcard Q firmware predating version 1.5.0Q
- Certain older versions of Coldcard's separate "Edge" firmware

Although later Coldcard models may have had greater randomness than affected Mk2 and Mk3 devices, Coinkite has described the issue as serious and recommends migration in most circumstances. Whether migration is necessary depends on the particular wallet and how it was originally created.

**Installing New Firmware Does Not Eliminate the Risk**

Coinkite has released corrected firmware for affected models. Installing the update corrects the problem only for newly generated recovery phrases going forward.

Importantly, updating the firmware does not repair a recovery phrase previously created with affected firmware. The weakness lies in the recovery phrase itself, not the physical device.

Likewise, importing the same recovery phrase into a different hardware wallet does not remove the vulnerability because the recovery phrase, not the physical device, controls access to the Bitcoin.

Coinkite recommends that affected users:

- Install the corrected firmware;
- Generate an entirely new recovery phrase; and
- Transfer Bitcoin to addresses controlled by the new wallet.

The company also recommends verifying the new wallet with a small test transfer before moving the remaining balance. Because even a correctly performed migration can result in the permanent loss of cryptocurrency, holders should proceed carefully and consider obtaining qualified technical assistance when appropriate.

**What Should Bitcoin Holders Do?**

Individuals and organizations holding Bitcoin should consider the following:



1. Determine which Coldcard model and firmware version were used when the wallet's recovery phrase was originally created.
2. Do not assume that installing a firmware update, changing a PIN, or moving the same recovery phrase to another wallet resolves the problem.
3. Never enter a recovery phrase into a website or provide it to anyone offering unsolicited assistance.
4. Review whether the wallet uses an additional passphrase, multiple independent signing devices, or another layer of protection.
5. Develop and carefully document a migration plan before moving substantial holdings.
6. Preserve transaction records, wallet information and related communications if funds have already been transferred without authorization.
7. Review insurance coverage, internal controls, fiduciary obligations, estate-planning documents and incident-response procedures to determine whether additional legal or operational steps may be appropriate.

Although this vulnerability concerns recovery phrases generated through affected Coldcard firmware—not a flaw in the Bitcoin network itself —it illustrates a broader point. Digital-asset security depends not only on the underlying blockchain, but also on the devices, software, recovery procedures, and people making decisions involved in controlling and safeguarding those assets.

Questions surrounding cryptocurrency custody, digital-asset security, and fiduciary responsibilities often involve a range of legal and practical considerations. If you have questions about the issues discussed above, including the use of a Coldcard wallet or the security of cryptocurrency held as part of your personal, business, trust or estate assets, please contact Brian McGovern at 856.673.3923 or bmcgovern@archerlaw.com.

## Related People


### Brian M. McGovern

Partner

bmcgovern@archerlaw.com

856.673.3923


## Related Services

- Corporate
- Private Wealth, Estates & Trusts