Ghost Tapping Scams Are on the Rise: What You Need to Know

As more people use tap-to-pay technology for everyday purchases, scammers have found a new way to exploit that technology in the form of ghost tapping. And while ghost tapping sounds like something out of a scary movie, it's a scam that can have very real consequences.

Tap-to-pay technology is designed to make payments quick and convenient. Whether you use a contactless bank or credit card or a smartphone wallet, the systems rely on near-field communication, or NFC, to send payment information when placed near a card reader. It's typically a faster, more secure way of paying that is protected by layers of encryption.

Unfortunately, criminals are always looking for new ways to take advantage of consumers and have begun to use contactless payment technology to steal money and personal data. In a ghost tapping scam, fraudsters use hidden card payment readers, fake terminals, or compromised devices to trigger an unauthorized contactless transaction. In some cases, they may try to get close enough to a person's wallet, pocket, or handbag to read a contactless card. In others, they use social engineering to trick someone into tapping their phone or card against a fake or altered payment terminal. Some scams may also involve stolen card details being loaded onto a fraudster's digital wallet and then used to make contactless purchases.

While the idea of someone stealing your money with a quick tap sounds frightening, most major banks and card providers have security systems that monitor unusual account activity, and many contactless transactions are limited in value. In addition, mobile wallets typically require facial recognition or a passcode before payment is approved. Still, there are steps consumers can take to help reduce the risk of falling victim to a ghost tapping scam, such as:

- Keep your cards and phone secure, especially in crowded places, such as airports, shopping centers, and public transportation.

- Be cautious if someone carrying a device gets unusually close to you for no obvious reason.
- See if your bank offers card controls through its online app and consider using contactless features only when necessary.
- Check your account regularly for fraudulent activity and set up fraud alerts with your bank or credit card provider so you are notified of any suspicious card activity.
- Consider using a wallet with RFID-blocking technology.

If you are targeted by a ghost tapping scam, contact your bank or credit card provider immediately and request that they freeze/cancel your card. You should also update any passwords that are linked to your banking and digital wallet accounts.

This content has been reviewed by FINRA.

Prepared by Broadridge Advisor Solutions. © 2026 Broadridge Financial Services, Inc.