KERN COUNTY ELDER NEWS

Monthly Information Article | Kern County DEAR/EDRT TEAM*
*(Dependent/Elder Abuse Review) Team/EDRT (Elder Death Review Team)

JULY 2024

PEER-TO-PEER SCAMS

Written By: Katie Carruesco
Targeted Outreach Specialist,
Department of
Financial Protection & Innovation

Designed and Managed By:
Kern County District Attorney's Office -
Victim Services Unit

Beware of Payment App Fraud

Following nationwide reports of scammers targeting Venmo users, Forbes says peer-to-peer (P2P) scams are on the rise. The new scam involves a scammer "accidentally" sending money to consumers on the P2P service and then asking for the money back.

The Department of Financial Protection & Innovation (DFPI) advises consumers to never send back the money. Instead, contact the P2P service about the error. Scammers often use stolen funds that Venmo and other P2P services will eventually flag as fraudulent. A common version of this happens when a scammer uses a stolen credit card number to deposit the funds into a consumer's P2P account. Eventually, the real holder of the credit card may actually get that payment reversed as a fraudulent charge. This means the innocent consumer who returns the supposedly accidental deposit to the fraudster will experience a debit from the credit card company, and any transferred funds will come from the consumer's P2P account balance.

Agency Partners

- Bakersfield Police Department
- California Dept. of Financial Protection & Innovation
- California Dept. of Insurance
- CSUB
- Dept. of Social Services Licensing
- GBLA
- Independent Living Center of KC
- Kaiser Permanente
- Kern Co. Aging & Adult
- Kern Co. BHRS
- Kern Co. Coroner
- Kern Co. District Attorney
- Kern Co. DA Victim Services
- Kern Co. Family Law Facilitator
- Kern Co. Public Health
- Kern Regional Center
- Kern Co. Sheriff's Office
- Kern Co. Veterans Service Dept.
- Social Security Admin.
- Strata Credit Union

P2P scams can take many other forms, including:

- Scammers impersonating a consumer's bank to alert them about “suspicious activity” on their account and direct them to send money to themselves or “the bank’s address” to reverse a transaction or to verify the account is not frozen.
- Fraudsters reaching out to consumers claiming to represent a fraud department or merchant and ask them to confirm information such as their bank account username and password, credit card or debit card data, or Social Security numbers.
- Scammers posing as a legitimate business requesting a P2P payment for a product or service.
- Scammers connecting a stolen credit card to a payment app then look for people selling big ticket items (such as a computer, tablet, or car) online. The scammers will offer to pay for the product using the app. Once the seller accepts the payment and sends the item, they’ll soon discover that the payment sent is not to a legitimate buyer, and the money collected is removed from their account. The seller is then without either the item or the money.
- Fraudsters sending spoofed emails warning that an account is about to be suspended and that the account holder must enter their password on a spoofed webpage.

When using these services, remember to never share personal information, treat P2P payments like cash, and not pay for products until they receive them. Victims of a scam involving P2P payment apps can file a complaint with the Federal Trade Commission.

To file a complaint against a P2P company, contact the DFPI, visit: https://dfpi.ca.gov/2023/05/24/how-to-file-a-complaint-with-the-dfpi/