U.S. Consumers Targeted in $1 Billion Scam Linked to Chinese Crime Rings

October 18, 2025 - A sophisticated wave of scam text messages, linked to criminal networks based in China, has defrauded Americans of more than $1 billion over the past three years, according to a recent report from the Department of Homeland Security. The scheme relies on simple but convincing messages sent to mobile phones, claiming the recipient owes a small toll, parking fee, or postal delivery charge. The messages often include a link to what appears to be a legitimate agency website, but itâ€™s a trap.

When victims click the link and enter personal or payment information, the data is quickly harvested and misused. Criminals then use that information to make unauthorized purchases or transfer funds through gift cards and digital wallets. Law enforcement officials say the stolen goods are often shipped overseas and sold for cash, making the fraud harder to trace and prosecute.

The people being targeted are everyday phone usersâ€”drivers, online shoppers, and even small business owners. Many victims say the texts felt plausible enough to respond to, especially when they seemed related to common services like toll roads or package deliveries. A growing number of Americans are only discovering the fraud after checking bank statements or receiving alerts about purchases they never made.

Behind the scenes, these scams are powered by what authorities call â€œSIM farmsâ€•â€”banks of mobile phones and SIM car operated by criminals to blast out hundreds of thousands of messages. Many of these devices are located in the U.S., making the texts appear more credible and harder to filter. According to a report in The Independent, these crime rings are recruiting gig workers to unknowingly assist in laundering the proceeds, often by purchasing goods or redeeming gift cards that are then routed abroad.

Federal officials, including the Department of Homeland Security, have warned that these scams are escalating in both volume and technical complexity. In some cases, criminals have been able to link stolen credit cards to mobile wallets, allowing them to spend quickly before victims or banks can intervene.

For consumers, awareness is the first line of defense. Experts recommend treating any unsolicited text about a payment or fee with suspicion, especially if it includes a link. Legitimate government agencies or delivery companies rarely, if ever, contact people through text messages asking for immediate payment. If you receive such a message, itâ€™s best to visit the agencyâ€™s official website directly or call a verified customer service number to check whether the notice is real.

If you think youâ€™ve been scammed, financial institutions urge you to contact them immediately to freeze or cancel affected cards. You should also report the incident to the Federal Trade Commission at reportfraud.ftc.gov.

While these scams may seem like just another digital nuisance, the scale and sophistication involved make them a serious threat to U.S. consumers. Staying cautious and verifying before clicking could be the difference between a normal day and a financial headache that takes months to untangle.