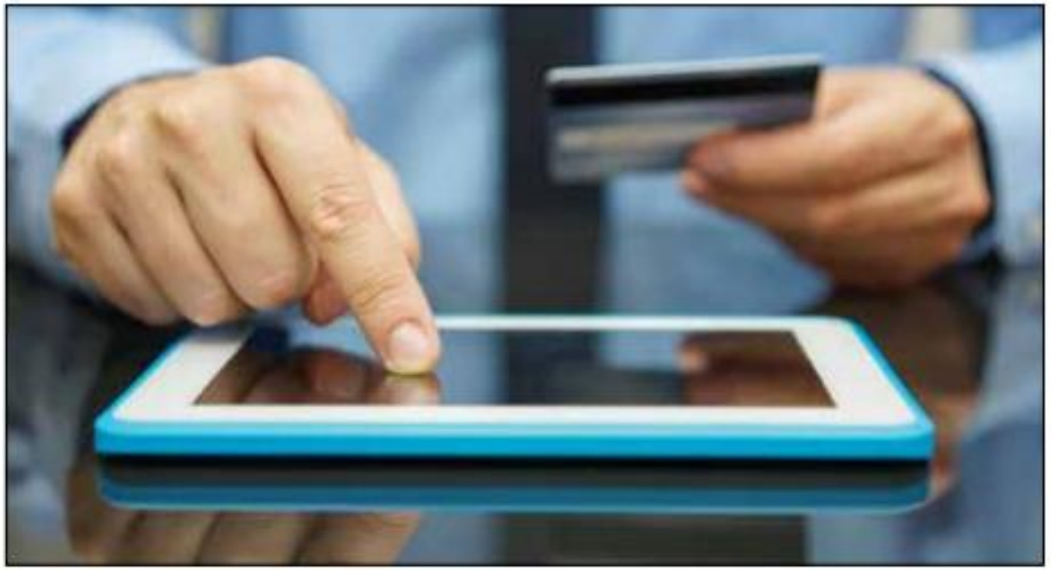
Snapped, cracked and popped: Preventing debit card fraud

By U.S. Army Capt.
Anouck McCall
Legal Assistance Attorney
JFHQ-NCR/MDW



What do your debit card, Instagram account and thousands of dollars have in common?

They could be part of a financial scam known as "card popping" or "card cracking" that predominantly preys upon students and young enlisted service members. The scheme may resemble the following:

A swindler on social media determines from any number of indicators (e.g., pictures, locations, usernames, handles, posts, connections, likes) that an individual is active duty military. He or she may then bait the subject with a public (and official reading) solicitation such as "For USAA Members Only." Upon clicking on the exclusive-sounding lure, the soon-to-be victim engages in direct messaging with the fraudster who – after brief pleasantries – offers the service member the prospect of quick cash. For instance, it could be under the guise of the scammer needing to lower his tax liability by transferring money or wanting to share a lucrative business opportunity whereby a large sum will be deposited into the service member's bank account on the promise that a portion will be returned to the con artist. At some point, the conversation may move to phone or text. Once the service member is hooked, the charlatan asks for the debit card and personal identification number (PIN) along with the associated online username and password. Once armed with these sensitive pieces of information, the thief proceeds to deposit checks either through a mobile application or automated teller machine (ATM). Before the checks clear (which they never will as they are fraudulent), the crook will overdraw the account against those bad checks. The service member is left responsible for the significant shortfall.

If this happens to you, your first thought may be to label yourself a victim of identity theft. While your identity was in fact stolen, you were actually complicit in the activity. In the eyes of the law, you too are a criminal and may be arrested and charged with fraud. You could face jail time and incur the expense of hiring a defense attorney. The parade of horrors hardly ends there: your financial institution will not only expect reimbursement, but will also likely terminate its relationship with you. In the event that it is USAA, being dumped as a customer means the loss of many near and long-term membership benefits including credit and low-interest loans as well as valuable products, namely insurance, banking, investment, retirement planning or savings on travel and shopping. Credit reporting agencies certainly will be notified, which will negatively impact your credit.

Further, you may face counseling or discipline from your command. If you hold a security clearance, it may be suspended; if a renewal is on the horizon, you will have to declare your misdeed and it could be an impediment to retaining your status.

Should you believe that you have been targeted by one of these financial villains, swiftly contact your banking institution and local law enforcement so they may mitigate potential losses and investigate the matter. Preserve as much evidence as possible – dates/times and screenshots of any exchanges combined with the trickster's Facebook, Twitter or Instagram username and/or phone number.

At first blush, making a fast buck is enticing. Who wouldn't want extra spending money for a new motorcycle or lavish shopping spree? As the Saturday Evening Post columnist, Franklin P. Jones, once said: "When you get something for nothing, you haven't been billed for it yet."

The cost of allowing someone to snap, crack, or pop your card is not worth it.