Police across the country have reported an emerging scam known as “Card Cracking” aimed predominantly at college students that involve debit card holders being solicited into providing their physical debit card as well as their Personal Identification Number (PIN) to the solicitor with the promise of payment in return. This payment is promised in the form of excess funds from a deposited check being left in the cardholder’s account. In addition to offering cardholders cash for participating in this scam and providing their debit cards and corresponding PIN numbers, cardholders have also been promised scholarship money and told to report their card stolen to avoid responsibility.

Solicitors have been telling victims they need a valid bank account so they (the solicitor) can deposit a check and withdraw cash. The solicitors tell the victim they will deposit a check for a certain amount and then withdraw a significantly less amount in cash, and promise the victim that they can keep the remaining money. Typically, solicitors have been asking to obtain the victim’s debit card in person at an agreed meeting place, or through the cardholder mailing the card to the solicitor.

Once the card and PIN number are obtained, the solicitor will deposit a counterfeit check into the victim’s account using an ATM, and then immediately withdraw a portion (typical promise is 50%) of the total amount of the check in cash.

Since there is a delay in the processing of most checks, the perpetrator has already retrieved the cash well before the financial institution discovers the check is counterfeit. The original card holder is then held liable to the financial institution for the stolen funds. Cardholders who willingly participate in this scam could also face criminal charges despite claiming they are the victims, based on the circumstances. Also, with the perpetrator using the cardholder’s PIN number, which is meant to be a security and authentication measure for the cardholder, it is difficult for the victim to claim unauthorized withdrawals.

This is seen by law enforcement and banking professionals as a new variation of fake-check fraud. This scam leaves the account holder vulnerable to depletion of legitimate funds they already had present in their account. For college students in particular, this could also lead to the depletion of funds present in their account including student loans, scholarships, and tuition reimbursements.

This scam could affect anyone, but police report that college students have been the main targets. The victims are typically approached and solicited through postings on various social media sites, including Facebook, YouTube, Instagram, and Craigslist. The perpetrators of this
scam are also known to hang-out at venues with a large presence of college students, and solicit these students for their debit cards and PIN numbers.

This scam is not exclusive to any one college campus and has occurred at various colleges throughout the country. Additionally, there is no single individual or group that is solely responsible for conducting this scam. There are many individuals and groups that are participating in this scam independent of one another.

**Safety Tips for Debit Card Holders:**

- **Always** verify the identity of the person trying to obtain personal information.
- **Never** give personal information to someone over the phone or via email. Personal information includes: Birth dates, social security numbers, maiden names, addresses, bank account numbers, debit/credit card numbers, PIN numbers, etc.
- Maintain a record of the phone call or solicitation. Write down the phone number that the person is calling from, the time and date they called, the caller’s name, and reported affiliation. If it was online, save a copy of the email conversation or advertisement.
- If it sounds too good to be true, it probably is.
- Report all suspicious people and circumstances to Campus Security and Police Services at (208) 426-6911 or from any blue phone.

 Anyone with information about incidents like this are asked to contact Campus Security and Police Services at (208) 426-6911, in person at the University Security Department located in Capital Village at 2245 University Drive; or, if you wish, anonymously through Silent Witness at [https://secureforms.boisestate.edu/security/](https://secureforms.boisestate.edu/security/).

Crime information can also be reported to Crime Stoppers by calling 208-343-COPS or 208-343-2677. You can remain anonymous and may be eligible for a reward up to $1,000 if your information leads to an arrest and filing of charges.