



OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



FINANCIAL SERVICES SECTOR

08 May 2020

LIR 200508002

“Cardless” Mobile Banking Applications Used in Account Takeover Fraud

The FBI’s Criminal Investigative Division (CID), in coordination with the FBI’s Office of Private Sector (OPS), prepared this LIR to inform the financial services sector about criminals using “cardless” automated teller machine (ATM) access code vulnerabilities to commit fraud and evade financial institution policy restrictions. Criminal actors exploit the existing mobile device ID security vulnerabilities to conduct account takeover and place illicit proceeds into the U.S. banking system. (See Graphic: Cardless ATM Transactions.)

Cardless banking provides convenience and security, while allowing account holders the ability to deposit, withdraw, and transfer funds through a financial institution's mobile banking application without using a bank card. However, criminals are anonymously conducting suspicious financial transactions at multiple ATM locations outside of the geographic footprint of the account holders.

- In 2018, cyber criminals used stolen cardless ATM access codes to deposit money obtained from an elaborate business email compromise (BEC) scheme. In 2017, the same group of criminals targeted and defrauded a U.S. construction company of more than \$1 million.
- In a series of 11 incidents, criminals used stolen cardless ATM access codes to deposit counterfeit checks into a U.S. bank account. The transaction notifications were sent to the legitimate account holder’s phone number, who was neither aware of the fraud, nor had they shared their bank information.
- A U.S. bank experienced more than \$100,000 in fraud losses through the use of cardless ATM access codes after funds were withdrawn from approximately 125 customer accounts at 17 different ATM locations in three different U.S. states. Four individuals were indicted for stealing bank customers’ usernames, PINs, and passwords.¹

The following indications separately do not accurately determine criminal actors’ use of cardless ATM access codes for illicit purposes and should be looked at in context. Organizations should evaluate the totality of suspicious ATM transactions and other relevant circumstances before notifying security/law enforcement personnel. These suspicious activities/indicators include, but are not limited to any individual, group, or business:

- Multiple requests for mobile access codes by the account holder;
- Re-occurring deposits of the same or similar amount;
- Multiple deposits outside of the geographic area of the account holder; or
- Rapid movement (i.e. wire transfers) of funds deposited into account.

If you notice or become aware of any such activity, contact your local FBI field office.

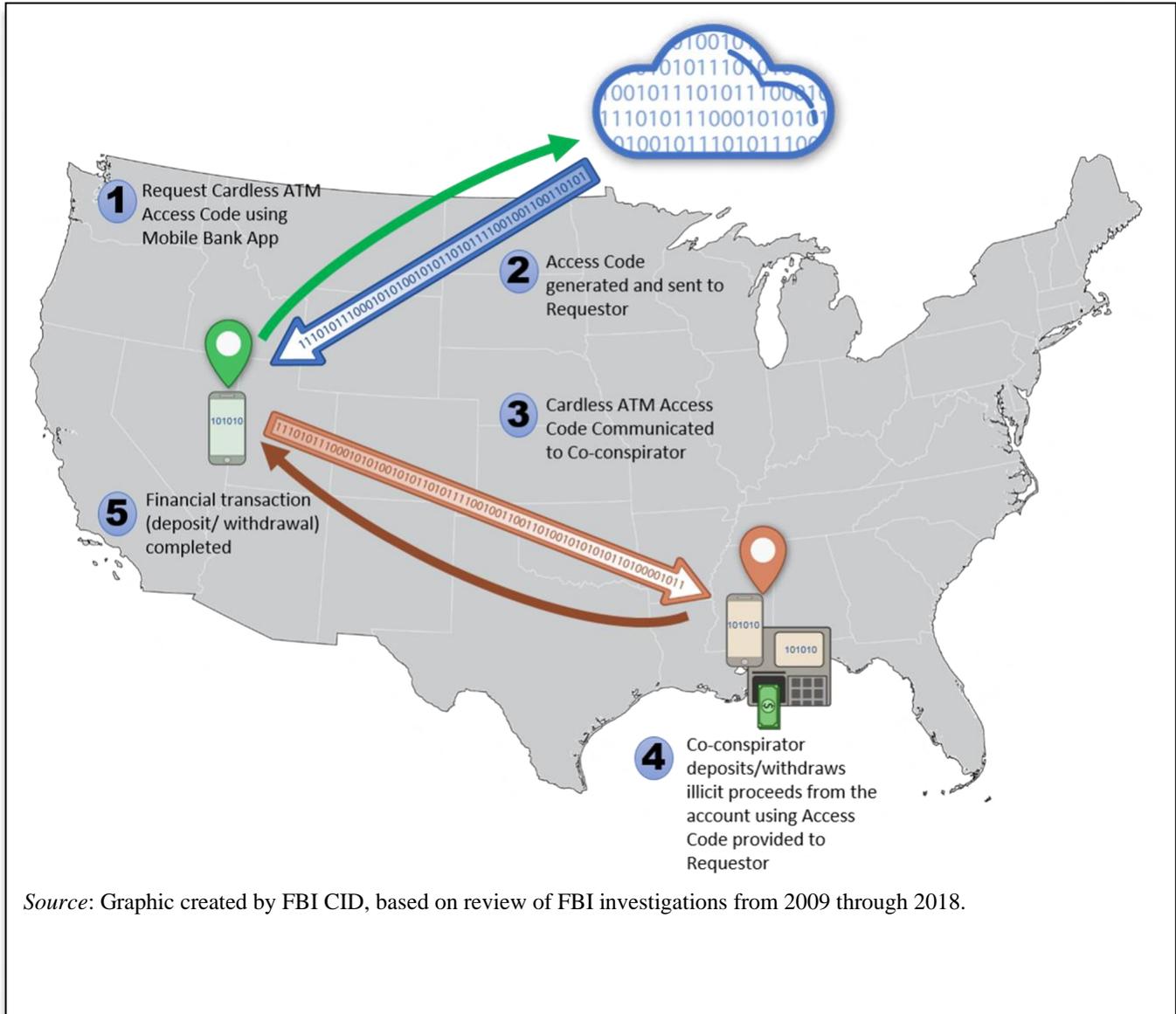


OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)



Cardless ATM Transaction Process



OPS's Information Sharing and Analysis Unit disseminated this LIR; please direct any requests and questions to your FBI Private Sector Coordinator at your [local FBI Field Office](#): <https://www.fbi.gov/contact-us/field-offices>.



Traffic Light Protocol (TLP) Definitions

Color	When should it be used?	How may it be shared?
<p>TLP:RED</p>  <p>Not for disclosure, restricted to participants only.</p>	<p>Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.</p>	<p>Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, TLP:RED should be exchanged verbally or in person.</p>
<p>TLP:AMBER</p>  <p>Limited disclosure, restricted to participants' organizations.</p>	<p>Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.</p>
<p>TLP:GREEN</p>  <p>Limited disclosure, restricted to the community.</p>	<p>Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.</p>	<p>Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. TLP:GREEN information may not be released outside of the community.</p>

¹ Online news article; WCPO.com; "Four indicted in 'cardless ATM' bank fraud scheme for bilking Fifth Third out of \$106K"; 9 November 2018; <https://www.wcpo.com/news/local-news/hamilton-county/cincinnati/four-indicted-in-cardless-atm-bank-fraud-scheme-for-bilking-fifth-third-out-of-106k>; accessed on 30 January 2019; The article is based on court documents.