



## OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

### FINANCIAL SERVICES SECTOR

12 April 2022

LIR 220412007

## Multi-State Check Thefts Targeting Religious Institutions and Exploiting Mobile Banking Applications, Consistent with Romanian Organized Crime Tactics

*References in this LIR to any specific commercial product, process, or service or the use of any corporate name herein is for informational purposes only and does not constitute an endorsement, recommendation, or disparagement of that product, process, service, or corporation on behalf of the FBI.*

The FBI Kansas City Field Office, in coordination with FBI Omaha, FBI Columbia, the Criminal Investigative Division, and the Office of Private Sector (OPS), prepared this LIR to alert the financial sector and religious organizations about the multi-state theft and fraudulent negotiation of checks made payable as donations to religious organizations. Based on arrest information since late 2020, known Romanian organized crime (ROC) tactics, and account openings with Romanian documents, this activity is most closely linked to ROC groups.<sup>a</sup> Thefts are generally successful, as donors expect their checks to clear and do not realize the church never received them until reviewing donation statements months later.

To facilitate the fraud, criminal actors open multiple financial accounts, often with fraudulent identification, and use ATM deposits and a remote capture deposit feature of mobile banking applications. As this scheme continues to yield profits, groups will likely extend their efforts to other states, resulting in millions of dollars in losses.

- In February 2022, a Romanian national received a five-year prison sentence as a co-conspirator who worked with a group to steal over 3,000 checks from US religious organizations' mailboxes in multiple states, resulting in over \$1.3 million dollars in losses to those organizations. The group used financial accounts opened under false identities and even recruited an insider at a financial institution to facilitate approximately 412 account openings.
- In January 2022, unidentified subjects targeted the mailboxes of at least three identified Kansas-based religious organizations and stole physical checks sent as church donations. The thefts from all three religious organizations occurred from January 2021 to February 2022. The checks were negotiated using mobile banking applications. Two of the three religious organizations did not use locks on their mailboxes.
- In January 2021, a financial institution froze a Romanian client's account due to fraud indicators after the individual used a mobile banking application to negotiate "hundreds" of donations by check taken from the mailboxes of religious organizations in Florida, North Carolina, and South Carolina.

<sup>a</sup> The FBI assumes unidentified criminal actors committing these thefts are also tied to ROC networks. If this proves false, indicators relating to the use of Romanian identification and known ROC tactics would need to be reconsidered.



## OFFICE of PRIVATE SECTOR

LIAISON INFORMATION REPORT (LIR)

- In October 2020, fraud actors presented Romanian passports and California state identification cards to open accounts at a Nebraska financial institution. They deposited checks stolen from religious and non-profit organizations into these accounts and then transferred the funds to other accounts.

### Romanian Traveling Crime Groups

Romanian traveling crime groups are mobile, financially motivated transnational ROC groups associated in the United States with multi-state strings of distraction theft and fraud incidents. These groups center on ethnic, family, and community associations and are agile, fluid, and project-based, frequently adopting new tactics or technologies to expand their criminal targets and profit base. In general, they operate in cells of two to eight persons as part of larger transnational ROC networks. They rarely remain in place long and make extensive use of false identification to avoid focused law enforcement attention. Often, they remit significant portions of their criminal proceeds to clan or family members in Europe, usually via webs of wire transfers, cross-border bulk cash smuggling, and concealment in shipped parcels. Criminal actors in these groups often claim asylum in the United States due to an established history of ethnic discrimination in Europe.

These groups engage in a myriad of criminal activities, including document and immigration fraud, human smuggling and trafficking, organized thefts, access device fraud, and money laundering. Some groups conduct ATM and credit card skimming and cash-outs, while others predominantly focus on distraction thefts, scams, or home invasions. Distraction theft targets are often elderly individuals, homeowners, and banks or retail stores. Such thefts can involve pickpocketing, jewelry swap schemes, organized distraction of store employees to facilitate shoplifting, subjects posing as utility workers or drivers in distress to gain access to private homes, and quick-change or shortchange scams, in which subjects engage a bank teller or store clerk in a confusing series of cash transactions, in the end convincing them to provide more cash in change than the subject is owed. While individual thefts often result in low-level damages, collectively they cause tens of millions of dollars in losses each year to US victims, victim institutions, retailers, and banks.

*Sources: A wide range of FBI-held federal, state and local law enforcement reporting and open-source articles.*

### Indicators for Business Owners and Religious Organizations

Business owners and religious organizations are encouraged to document individuals who display suspicious behavior, including but not limited to the following indicators. These indicators singularly may not be indicative of criminal behavior but should be considered in their totality.

- Signs of tampering with locks, mailboxes, or donation areas,
- A sudden decrease in expected donations or missing serial donations from known members,
- Businesses or church members receiving copies of checks altered from their original state,
- Visitors inquiring about religious services or attempting to “tour” facilities,
- Visitors showing up for a singular service and not returning,



- Small groups (one to three) individuals, possibly with children, loitering near the church premises, especially engaged in panhandling or pandering of jewelry, as these activities may provide cover for them to observe church premises for operational planning purposes, and
- Occupied vehicles (usually minivans and sports utility vehicles) observed in the area for long periods with no obvious purpose, especially those displaying out-of-state or temporary tags.

Religious institutions are further encouraged to closely monitor recurring or anticipated donations in order to promptly identify discrepancies. An increase in public reporting of pickpocketing or distraction theft activities in the area should also be considered a possible indicator of these ROC groups' presence.

### Indicators for Financial Institutions





Financial Institutions are encouraged to be aware of and document individuals who display suspicious behaviors consistent with the facilitation of donation theft, including but not limited to the following indicators. These indicators singularly may not be indicative of criminal behavior but should be considered in their totality.

- A sudden or steep rise in the use of Romanian or other foreign identification to open new accounts,
- The use of newly issued, out of state identification to open new accounts,
- Attempts to open a new account with other individuals directing or speaking on behalf of the account opener during the process,
- Individuals promptly transferring funds from a newly opened account to other accounts using remote and/or ATM check deposits,
- Deposits are out of pattern with a personal account and only occur after normal business hours, and
- Accounts being opened in the names of individuals other than the depositor of the fraudulent checks.

This LIR was disseminated from OPS's Information Sharing and Analysis Unit. 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):  
<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><b>TLP:RED</b></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><b>TLP:AMBER</b></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. <b>Sources are at liberty to specify additional intended limits of the sharing; these must be adhered to.</b></p>
<p><b>TLP:GREEN</b></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>
<p><b>TLP:WHITE</b></p>  <p>Disclosure is not limited.</p>	<p>Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.</p>	<p>Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.</p>