

**FINANCIAL SERVICES SECTOR****14 MARCH 2025****LIR 250314008****Warning of Increasing Robbery Risks to ATM Technicians**

*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's Criminal Investigative Division, in coordination with the Office of Private Sector (OPS), prepared this Liaison Information Report (LIR) to warn companies in the financial services sector about new ATM robbery tactics and the increased safety risks to ATM technicians. Due to improved ATM security, technology, and placement, some criminals may be shifting to new ATM robbery tactics, whereby the technician inadvertently does the most difficult part of the theft: opening the machine.

Since 2021, ATM technician attacks have more than doubled. In some cases, criminals sabotage the ATMs and wait for service technicians to arrive. As the technicians open the ATM, the criminals threaten or assault the technician and subsequently steal the ATM cash cassettes. Additionally, criminals are reportedly following ATM technicians from their homes or between jobs and robbing them at non-sabotaged machines. These new techniques have had a high success rate, with some incidents resulting in the theft of hundreds of thousands of dollars.

The following activities are potential indicators of imminent criminal activity. A single indicator does not accurately predict ATM technician assault or ATM theft; financial organizations should consider the totality of facts and circumstances before reporting to security/law enforcement personnel.

- Repeated sightings of the same vehicle following technicians from job to job or from home to job;
- Occupied vehicles not parked in marked parking spaces idling near ATMs, particularly vehicles idling for an extended period; and
- Obvious signs of ATM sabotage (for example, sticky substances blocking card slots, cards glued into slots, damage to keypads or screens, damaged or jammed cash dispensers).

Companies in the financial services sector should consider training ATM technicians, including those accompanied by private security guards, on some of the following mitigation techniques:

- Upon observing unusual activity potentially indicative of criminal activity at an ATM, technicians should:
  - Immediately suspend the service call;
  - Do not open the ATM;



## OFFICE of PRIVATE SECTOR

### Liaison Information Report (LIR)

- Enter the branch to alert the bank manager on duty, or enter the closest occupied building if servicing a standalone machine;
- Contact local law enforcement, alert them to the possibility of a robbery, and request officer assistance;
- Wait in a safe location for the police officer to arrive, then repair the ATM; and
- Hand over all evidence to the responding police officer.
- If ATM technicians notice they are being followed in transit to or from an ATM service location, they should contact emergency services and head toward the nearest police or fire station.





This LIR may be read in conjunction with LIR 240925002A, “Robbery Crews Use Multiple Techniques to Target ATM Service Technicians in Virginia,” dated 25 September 2024; LIR 231229010, “Robbery Crews Assault ATM Repair Technicians to Maximize Profit,” dated 29 December 2023; LIR 231204010, “Traveling ATM Robbery Crews Shift Tradecraft to Include Surveilling Robbery Targets,” dated 4 December 2023; and LIR 220502002, “Threat Actors Targeting Automated Teller Machine Technicians in the United States,” dated 2 May 2022.

The FBI’s Office of Private Sector 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**

<b>Color</b>	<b>When should it be used?</b>	<b>How may it be shared?</b>
<p><b>TLP: RED</b></p>  <p>For the eyes and ears of individual recipients only, no further disclosure.</p>	<p>Sources may use TLP: RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved.</p>	<p>Recipients may therefore not share TLP: RED information with anyone else. In the context of a meeting, for example, TLP: RED information is limited to those present at the meeting.</p>
<p><b>TLP: AMBER</b></p>  <p>Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. Note that <b>TLP: AMBER+STRICT</b> restricts sharing to the organization only.</p>	<p>Sources may use TLP: AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved.</p>	<p>Recipients may share TLP: AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization <b>only</b>, they must specify TLP: AMBER+STRICT.</p>
<p><b>TLP: GREEN</b></p>  <p>Limited disclosure, recipients can spread this within their community.</p>	<p>Sources may use TLP: GREEN when information is useful to increase awareness within their wider community.</p>	<p>Recipients may share TLP: GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP: GREEN information may not be shared outside of the community. Note: when “community” is not defined, assume the cybersecurity/defense community.</p>
<p><b>TLP: CLEAR</b></p>  <p>Recipients can spread this to the world, there is no limit on disclosure.</p>	<p>Sources may use TLP: CLEAR 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: CLEAR information may be shared without restriction.</p>