



## OFFICE of PRIVATE SECTOR

### Liaison Information Report (LIR)

## FINANCIAL SERVICES SECTOR

30 SEPTEMBER 2026

LIR 260930012

### Criminals Exploit Property Titles to Secure Illegitimate Loans

*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 prepared this Liaison Information Report (LIR) to inform the financial services sector about a home title theft scheme that exploited property title and hard money lending processes. The scheme relied on identity theft, homeowner impersonation, and knowledge of the home title and hard money lending process, which enabled perpetrators to recruit and embed complicit personnel in the financial and real estate industry, fraudulently gain control over home titles without the homeowners' knowledge, secure fraudulent hard money loans against mortgage properties, and distribute and launder the fraudulent proceeds. Actors frequently targeted unencumbered (without loans or liens on them) properties, which reduced scrutiny during verification and enabled faster loan approval.

On 19 March 2026, 11 individuals, including two foreign nationals, were arrested for a home title theft scheme, which resulted in approximately \$6 million in losses, with an intended loss of approximately \$17 million. Between January 2021 to May 2023, these actors allegedly secured fraudulent loans against residential properties in Los Angeles County, California, victimizing at least three property owners and four private money lenders. The scheme involved the following process:



Complicit mortgage brokers identified unencumbered properties, including secondary homes and those owned by elderly individuals. Actors then obtained homeowners' PII through ruses or mail theft and used the information to forge or alter identity documents.



Actors created email accounts impersonating homeowners and used stolen PII and fraudulent IDs to pose as agents, brokers, or relatives. In coordination with complicit brokers and a notary, actors submitted fraudulent loan applications and completed notarization using impersonators.



After securing loans, actors moved proceeds from escrow accounts to domestic shell business accounts opened with synthetic identities. Actors then layered transactions across multiple institutions and distributed funds among co-conspirators.



## OFFICE of PRIVATE SECTOR

### Liaison Information Report (LIR)

The following suspicious activities are potential indicators that an individual is attempting to conduct home title theft. A single indicator does not accurately identify fraudulent behavior; organizations should consider the totality of facts and circumstances before reporting to security or law enforcement personnel.

- Individual presents documents, including property deeds or death certificates, that appear altered or fraudulent;
- Individual presents personal identification that appears suspicious or fraudulent to secure a loan;
- Individual provides contact information on loan documentation that does not align with existing customer records;
- Individual takes out hard money loans against an unencumbered property, abandoned property, vacation or secondary home, or property owned by an individual who is elderly, disabled, or disadvantaged;
- Individual insists on conducting business virtually, particularly via email, rather than in person;
- Individual delays or avoids phone calls using contact numbers provided in the loan documentation;
- Individual conveys a sense of urgency to close on the loan;
- Individual makes urgent, last-minute requests to redirect escrow to disburse funds to a different account; and
- Individual poses as a “spokesperson” for the homeowner, claiming to be a relative (for example, a cousin or niece/nephew), especially if the purported homeowner is elderly.

Financial lenders that issue hard money loans, including private lenders and hard money brokers, are encouraged to take the following mitigation measures to identify and prevent this type of fraud:

- Meet loan applicants in person and verify identities using trusted records. Independently confirm claims of death or third-party representation.
- Verify property titles through county public records and/or an independent title company.
- Validate contact information, including phone numbers and email addresses, on loan documentation to ensure it matches existing customer records.
- Use internal or vetted notary services, and verify notary credentials and documentation.
- Confirm escrow disbursement instructions, and validate the relationship between the homeowner and recipient accounts prior to releasing funds.

If your organization has information on individuals conducting similar home title and hard money loan fraud schemes, please contact your local FBI Field Office and report the details regarding the incident to the FBI’s Internet Crime Complaint Center (IC3) at [www.IC3.gov](http://www.IC3.gov).



## OFFICE of PRIVATE SECTOR

### Liaison Information Report (LIR)

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>.

*This product was prepared by the FBI's Los Angeles Field Office and Criminal Division, in coordination with the Office of Private Sector.*

### Traffic Light Protocol (TLP) Definitions

| Color                                                                                                                                                                                                                                                                                                                   | When should it be used?                                                                                                                                                                            | How may it be shared?                                                                                                                                                                                                                                                                                                             |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>TLP: RED</b></p>  <p>For the eyes and ears of individual recipients only, no further disclosure.</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.                      | 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><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> | 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. | 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><b>TLP: GREEN</b></p>  <p>Limited disclosure, recipients can spread this within their community.</p>                                                                                                                              | Sources may use TLP: GREEN when information is useful to increase awareness within their wider community.                                                                                          | 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.                          |