Taking a fraud call

Last Modified on 11/23/2026 1:14 pm EST

Reader group: Member service
In a live knowledge base, only signed-in member service reps would see this page. It's public in this demo so you can explore.

First, protect the account

1. Verify the caller's identity using our standard questions. Never use information the caller offers first.
2. Block the affected card and issue a new one.
3. If online banking may be compromised, reset the member's credentials and end active sessions.

Then, open a dispute

1. Write down the date the member first told us. Reg E timelines start from this date, even if it was a voicemail.
2. Open a dispute case for each unauthorized electronic transaction.
3. Tell the member what happens next. See the Reg E dispute timeline.

Was the member tricked into sending the money themselves? Note it in the case. Authorized scam payments are handled differently from unauthorized transactions, and the compliance team will advise.

Support the member

Being scammed is upsetting and often embarrassing. Reassure the member that they did the right thing by calling, and share Spot common scams.