

# Verify identity before you reset MFA

Reset MFA is one of the most powerful actions in Ark. **Every request for one warrants investigation, never simple fulfillment.** Here is when a reset is appropriate, and how to confirm a request is real before you act on it.

## A reset drops the user to a single factor: their email

MFA protects an account because inbox access alone is not enough to get in. A reset removes that protection: until the user enrolls again, their email is the only thing standing in the way. If that inbox is already compromised the chain closes fast. The attacker gets the enrollment link, registers their own authenticator, then resets the password to the same inbox. **Everything that user can see and do in Ark is now theirs.**

01

Inbox already  
compromised

02

MFA reset performed

03

Enrollment link received

04

Attacker registers own  
MFA

05

Password reset, full  
access

### Start here: most requests need no reset

If the user still has the factor on file, they can add a second method themselves and no single-factor window ever opens. Someone moving to an authenticator app should use their existing phone MFA to register it, then retire the old method. Point them there first.

### When a reset is warranted

- The device holding the authenticator is lost, stolen, or unusable.
- The device was replaced or wiped and the authenticator was never migrated.
- The registered phone number is ported, cancelled, or out of service.
- The authenticator app was deleted, or its data was lost in a restore.

### Verifying the requester

- **Use a channel already on file**, not the one the request arrived on. A call to a known number is the strongest check available to you.
- **Never confirm by replying to the requesting email.** If that inbox is the problem, you are asking the attacker for permission.
- Ask something only the real user would know from their own activity in Ark.

### Treat these as warning signs

- Urgency or pressure, particularly near a distribution or capital call date.
- **Any request that arrives alongside, or shortly before, a change to bank or wire details.** That pairing is a well-worn fraud pattern, not a coincidence.
- A reply address that differs subtly from the one on file.
- A new phone number or email offered as part of the same request.

#### WHAT ARK DOES ON EVERY RESET

##### Every reset is audited

Ark records who initiated it, the user it applied to, and when. Those records are retained and reviewable.

##### Confirmation is your sign-off

The prompt requires you to type the action out in full. Completing it confirms you have verified the requester's identity.

**Use this feature lightly.** It exists to resolve genuine lockouts. Where identity has not been confirmed, no action is the safest action. Questions: [product@arkpes.com](mailto:product@arkpes.com)