Ruko

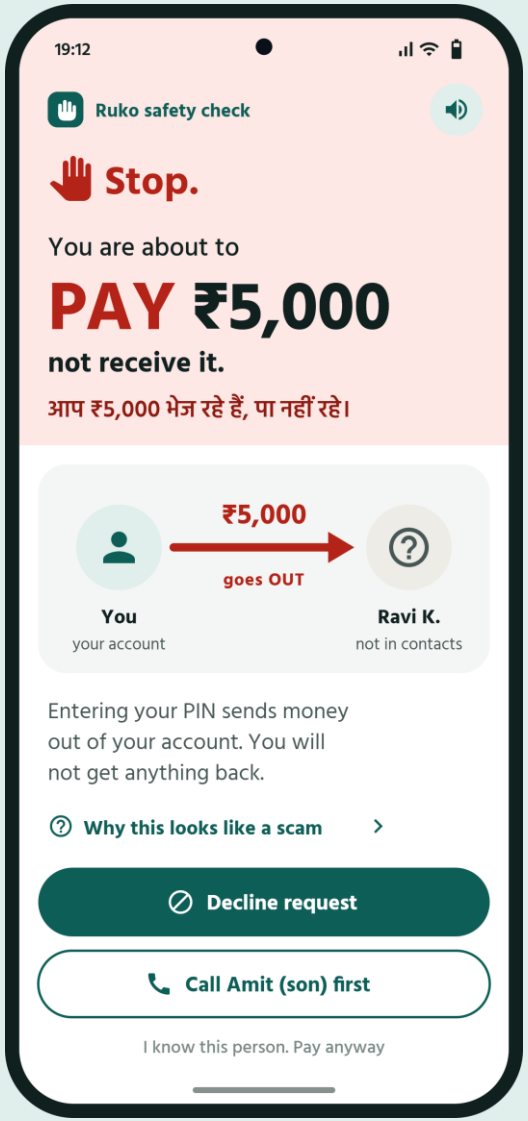
UX case study · 2026

A warning people believe, at the second it matters.

Scammers rush parents into paying. Ruko is a safety layer inside a payment app that pauses the payment, says plainly what will happen to their money, and puts family one tap away.

Nabaskar Brahma
Solo researcher and designer

Oct 2026 · 6 interviews with parents and relatives aged 48 to 68



Parents knew the rules. Under a scammer’s pressure they forgot them, so the warning has to arrive at that second.

01

The problem

Scammers keep parents on the phone and rush them. Today’s warnings look like every other pop-up, so they get tapped away.

02

What I did

6 interviews with relatives aged 48 to 68: their scams, who they trust, and a test of three warning messages.

03

What I designed

Ruko: a stop screen that names the money, explains why in their language, and offers one tap to call family.

> “If this exact message had popped up on my screen last year… my ₹4,000 would still be in my pocket today!”

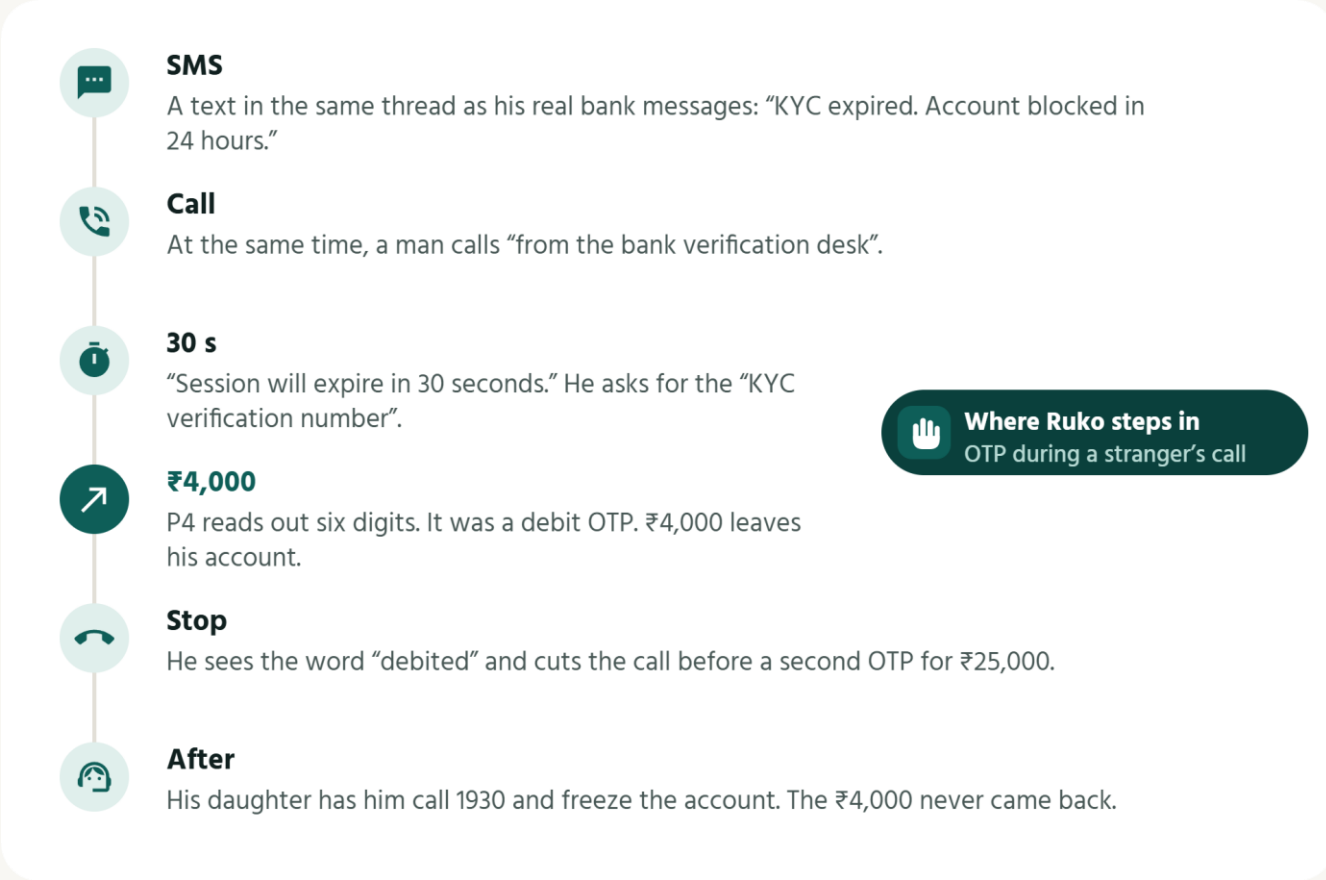
P4, family friend, 61, on the warning that names the OTP trap

He knew banks never ask for an OTP. With 30 seconds on the clock, he read one out.

30 s

P4, a retired officer, was told his bank KYC had expired. A caller asked for the “KYC verification number”.

> “In that moment of panic, you forget the rule that ‘banks never ask for OTP.’”
>
> P4, family friend, 61



Six conversations with family aged 48 to 68: close enough to be honest, too close to be neutral.

P1 Aunt, 52 — No loss

UPI: Daily

Fake electricity-bill SMS and call: pay a ₹10 “charge”

P2 Uncle, 56 — No loss

UPI: Daily, runs a shop

Fake buyer: scan a QR “to receive ₹8,000”

P3 Aunt, 48 — No loss

UPI: Sometimes

Prize message: ₹2,500 fee to claim ₹25 lakh

P4 Family friend, 61 — Lost ₹4,000

UPI: Sometimes

Fake bank KYC text and call: read out an OTP

P5 Grandmother, 68 — No loss

UPI: Rarely, family pays

Fake police call about her grandson: send ₹30,000

P6 Uncle, 64 — No loss

UPI: Rarely, prefers cash

Fake customs “digital arrest” call, scam texts weekly

How 30-minute talks in Hindi and English, about real payments and real scams, then three test warnings read aloud (in Hindi for P5).

Strength and bias They told me what they’d never tell a stranger, like P4’s loss. But it is one family circle, found by referral, and they may have been kind to my ideas.

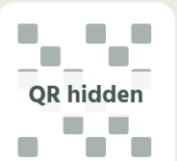
All 6 had met a scam. Fake “account blocked” texts and fake officers on the phone led.

Met it themselves (of 6)		Heard of a loss
Fake bill, KYC or “blocked” text	3 · P1 P4 P6	
Fake officer on the call	3 · P4 P5 P6	₹1.5 lakh
“Enter your PIN to receive”	1 · P2	₹50,000
Relative in trouble	1 · P5	₹50,000
Prize or job “fee”	1 · P3	₹3,000
Asked to read out an OTP	1 · P4	
Payment link from a fake supplier	0	₹18,000

One scam can carry several patterns. Each loss story counted once.

Fake buyer on WhatsApp
Number hidden

“I am sending ₹8,000 advance... Scan this QR & enter your 4-digit UPI PIN to RECEIVE ₹8,000 directly in your bank. Stay on call while scanning, link expires in 2 minutes.”



Redrawn, P2

Bank-style sender (spoofed)
Redrawn, P4 · account digits hidden

“Dear Customer, your [bank] A/c and UPI will be suspended today due to pending PAN KYC. Update at [link removed]”

“Txn of INR 4,000.00 on A/c [hidden] initiated... Do not share with anyone. OTP is ••••••”
Read out as a “KYC verification number”

Every scam borrowed something real: an official look, a ticking clock, a live call.

4 of 6

An official look

“an army uniform photo... makes you respect the person”

P2

4 of 6

A ticking clock

“Sir session will expire in 30 seconds”

P4

3 of 6

Staying on the call

“He stayed on the phone line continuously”

P2

2 of 6

Timing from real life

“just two days before, your uncle had paid the bill online”

P1

2 of 6

Renaming the risky step

A debit OTP, called a “KYC verification number”

P4

2 of 6

Keep it secret

“don’t tell anyone in your neighborhood”

P3

6 of 6 trust family first. The app is trusted only when it explains itself.

Trusted most → Not trusted

FIRST CALL

Family **6 of 6**

Son, daughter, grandchild, husband

“My son first.”
P1

“I only trust family.”
P5

TRUSTED, WITH CONDITIONS

The app **3 of 6**

“if it actually locks the transaction and explains clearly why” P2

The bank, in person **2 of 6**

Branch visit (P1, P4)

WHEN NO ONE IS HOME

People nearby **3 of 6**

Shop staff (P1, P2), a neighbour (P5)

NOT TRUSTED

A text that says it’s the bank
P4, P6

A bank logo on a chat profile
P1

Helpline numbers from search
P4

English pop-ups
P1, P5

“I don’t know what ‘the app’ or ‘the phone’ is thinking, I only trust family.” P5, grandmother, 68

I thought the gap was knowing the rules. It was remembering them under pressure.

My assumption: people fall for scams because nobody told them the rules.

2 of 6

knew the exact rule and still nearly or actually fell for the scam (P2, P4)

> “I have seen it 100 times, yet when that Army fellow was pressuring me on the call, my brain didn’t read the top banner!”

P2, on the app’s “Never enter UPI PIN to receive money” banner

What changed

Ruko is not an awareness feature. It repeats the rule at the second it is being broken, on the screen where it is being broken.

Asked which warning would stop them, 6 of 6 named the one that says where the money goes.

Warning 1
Generic

"Warning: this may be a fraud. Do not proceed."

0 of 6
chose it

P1 P2 P3 P4 P5 P6

3 would dismiss it
2 would freeze
1 would stop (P6)

Warning 2
Names the money

"Stop. You are about to PAY ₹5,000, not receive it. Entering your PIN sends money out of your account."

6 of 6
named it as one that would stop them

P1 P2 P3 P4 P5 P6

"This is 10 out of 10. It directly breaks the hypnosis." P2

Warning 3
Names the trap, offers a person

"This person asked for your OTP. Banks never ask for OTP. Call [son] before continuing?"

5 of 6
named it as one that would stop them

P1 P2 P3 P4 P5 P6

First choice for P3 and P5.
"like getting oxygen" P5

Each person heard all three, said what it meant and what they'd do, then which would stop them and which they'd ignore. Some named two.

Generic warnings get a reflex, not a reading.

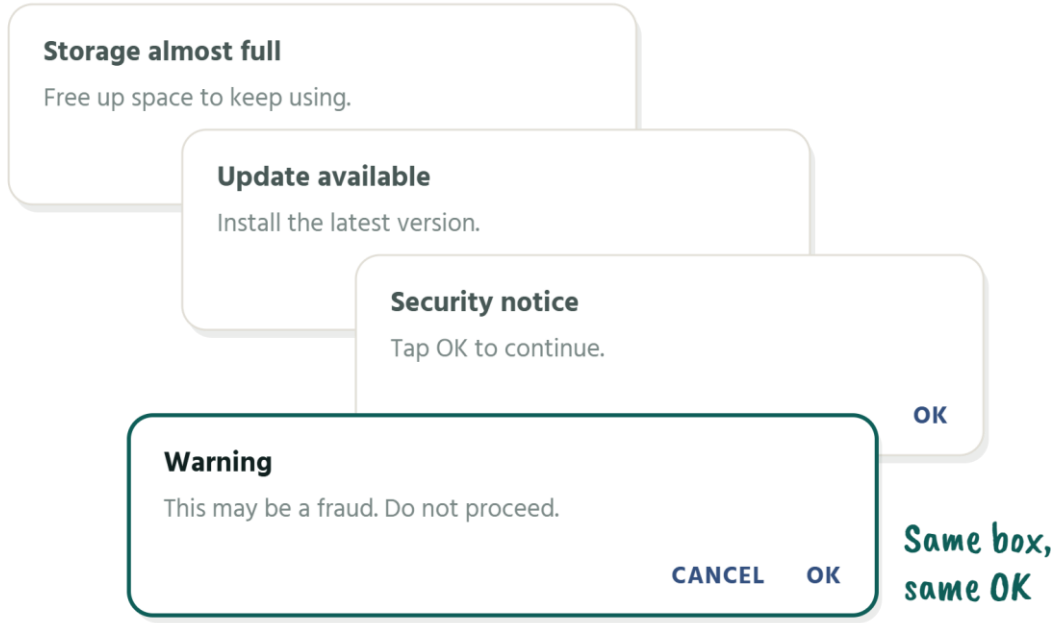
"phones write so many things in English every day… So we get the habit of pressing 'OK' without reading deeply."

P1, aunt, 52, pays daily

0 of 6 chose the generic warning

5 of 6 describe a habit for clearing pop-ups: tap OK, skip, close the app, press Back

3 of 6 struggled with English wording like "proceed" (P1, P3, P5)



A person, not a pop-up, ended 4 of the 6 scams.

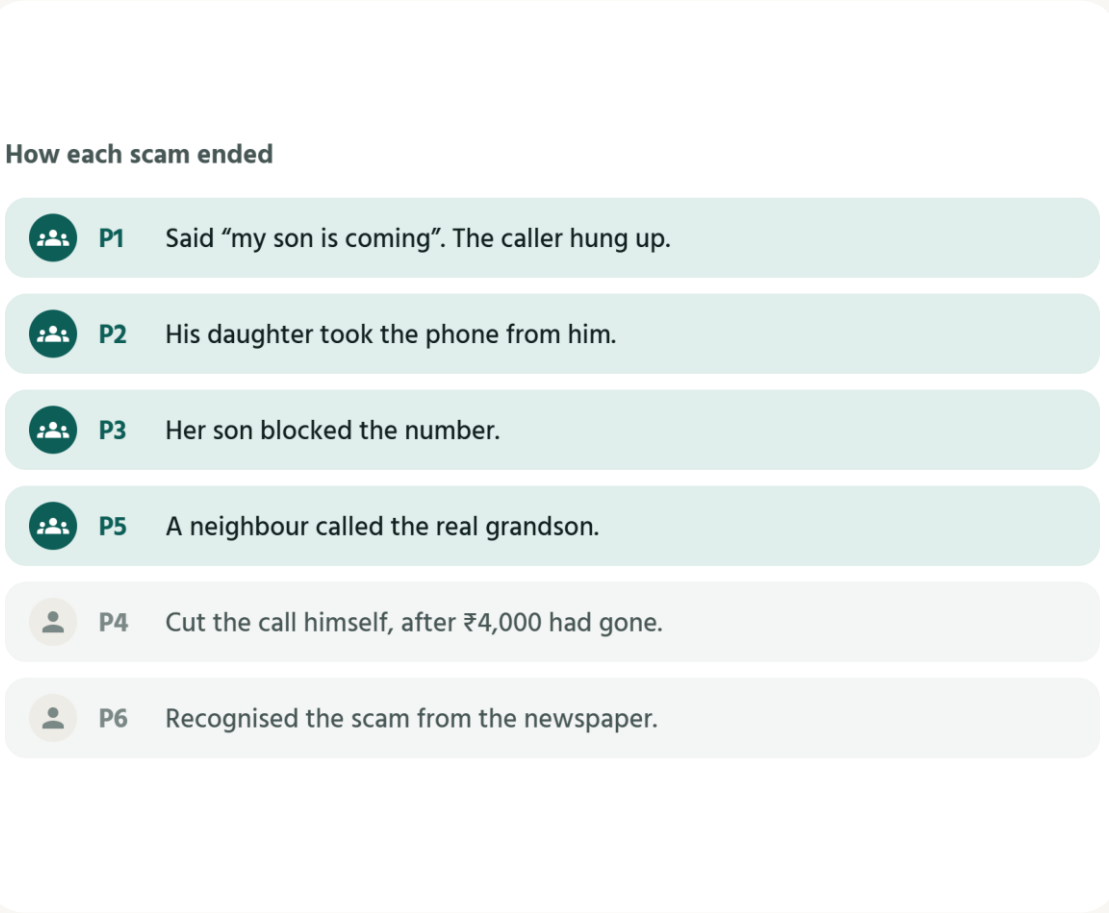
"seeing my grandson's name on the screen is like getting oxygen. I will press that button immediately."

P5, grandmother, 68

4 of 6 scams were ended by another person, or the mention of one

6 of 6 trust family first

2 of 6 mention scammers demanding secrecy (P3, P6)



The amount can’t spot a scam. The live call can.

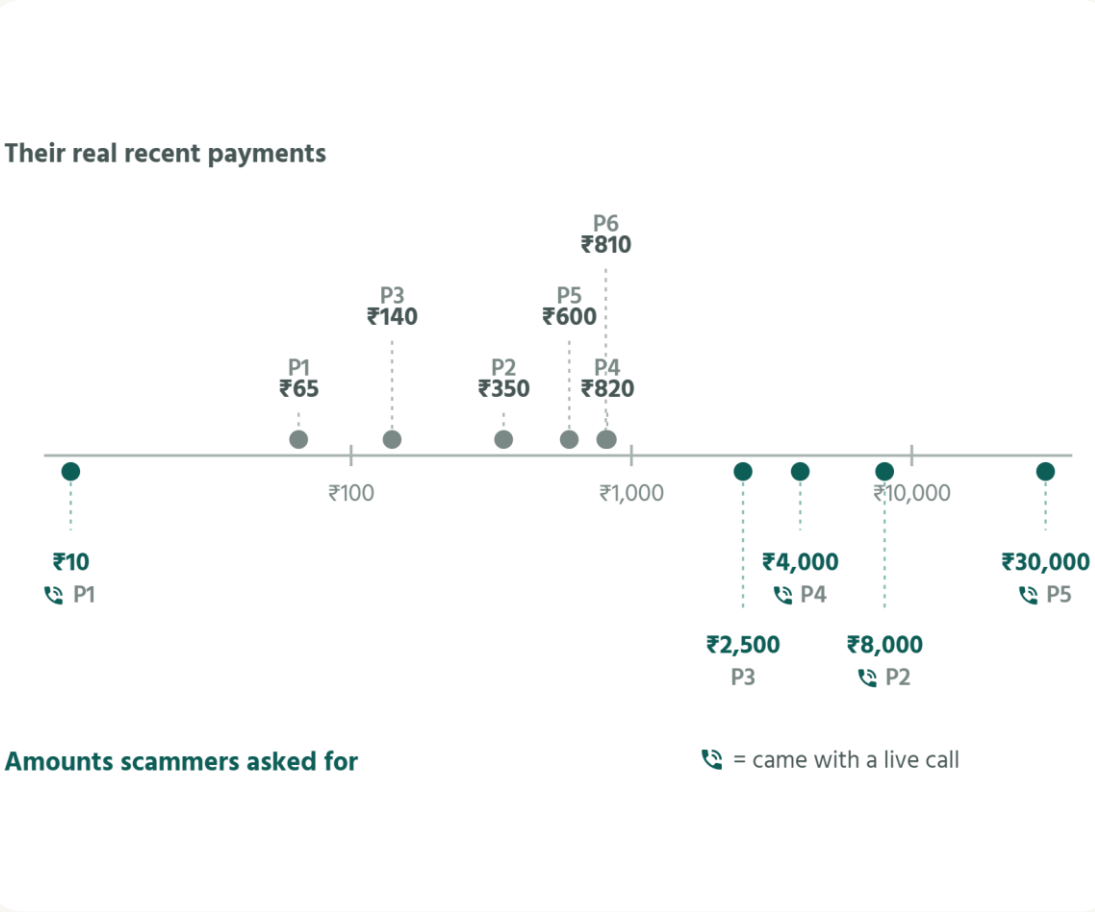
“Never allow a collect request or QR scan from WhatsApp to work while a person is actively on a phone call with an unknown number.”

P2, uncle, 56, runs a shop

5 of 6 scams ran over a live phone call

₹10 the smallest ask (P1), less than any of their real recent payments

3 of 6 don’t want checks on small or routine payments (P1, P2, P4)



Three rules every warning screen had to pass.

1

Say what will happen to the money, in their words.

From the warning test: 6 of 6

"PAY ₹5,000, not receive it." In Hindi, and read aloud on request.

2

Offer a person, not just a warning.

From insight 2: 5 of 6 chose it

"Call Amit first", by name, while the payment waits.

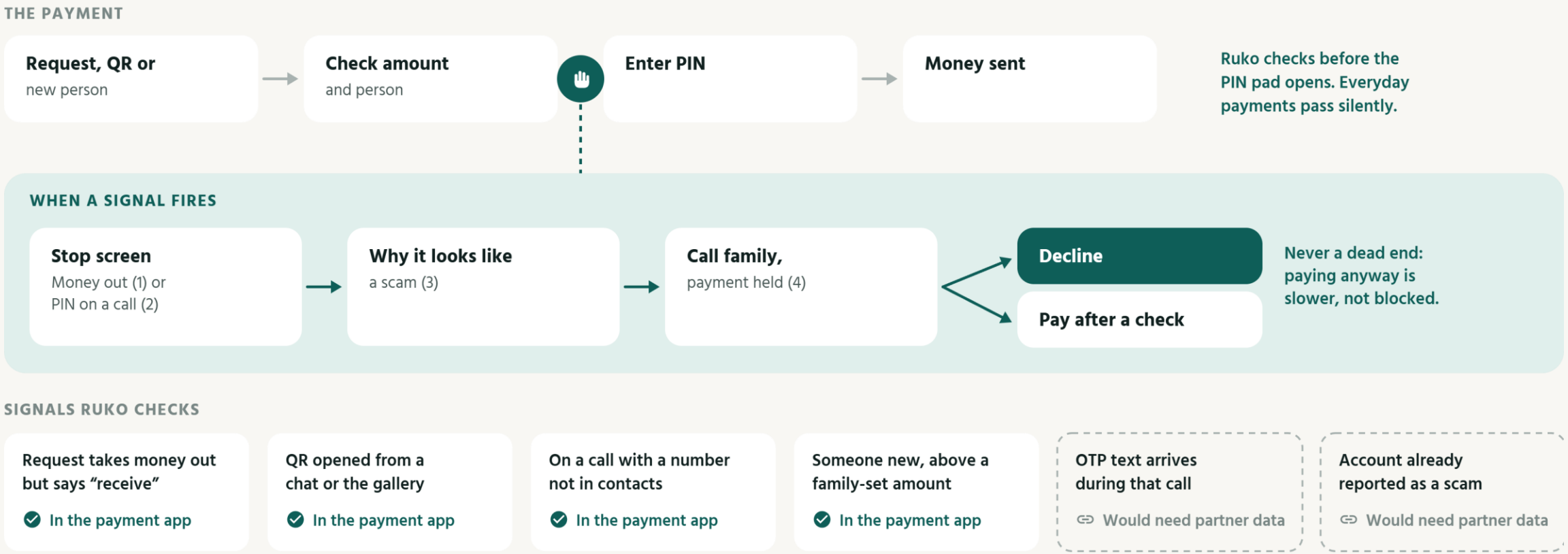
3

Step in at the risky moment only.

From insights 1 and 3

On a call with an unknown number, yes. On the ₹65 ironing bill, never.

Ruko checks once, just before the PIN, and stays silent for everyday payments.



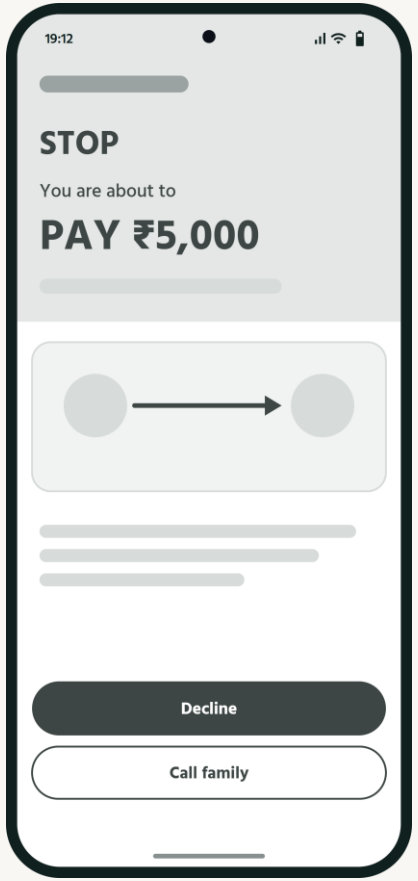
Before: set up once with family (5). After: if money is lost, get help (6).

A bottom sheet looked like every other pop-up. A full-screen stop won.



A · Bottom sheet

Slides over the payment. Lighter, but the Pay screen stays visible behind it.



B · Full-screen stop

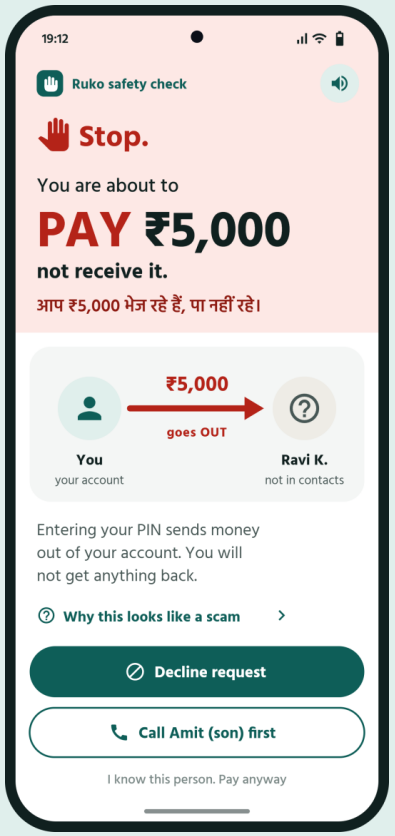
Takes over the screen. The amount and its direction are the only thing to read. Chosen.

> P2: "if it looks like an advertisement banner at the top or bottom of the screen, my eyes skip right over it."

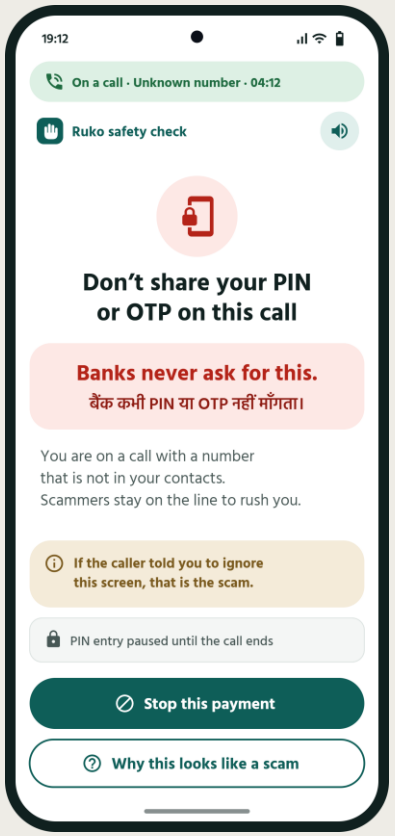
> P3 panics over "which button is safe?" One screen, one safe button.

> Full screen only for the stop moment, so it never becomes wallpaper.

Name the money and its direction. Say the rule at the second it is broken.



1 · Request takes money out



2 · PIN asked during a call

"PAY" in red and the amount huge. "If I read that ₹5,000 is going OUT of my bank, my hand will stop." (P1)

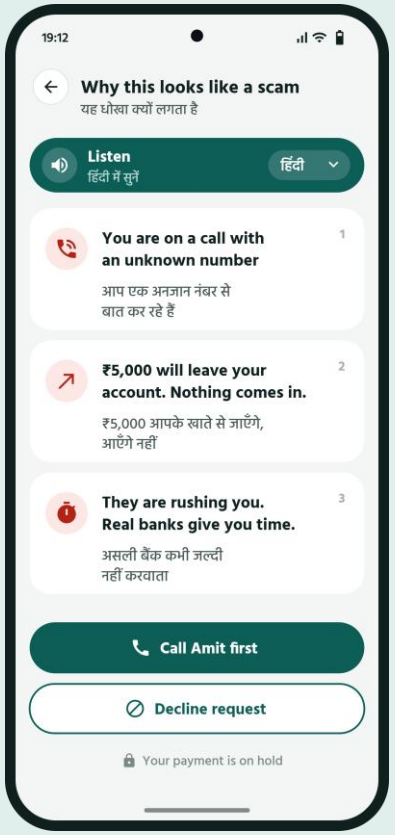
An arrow shows which way the money goes, for anyone who reads little English.

Decline is the big button, in the same place every time. P6: "Keep the buttons in one fixed place."

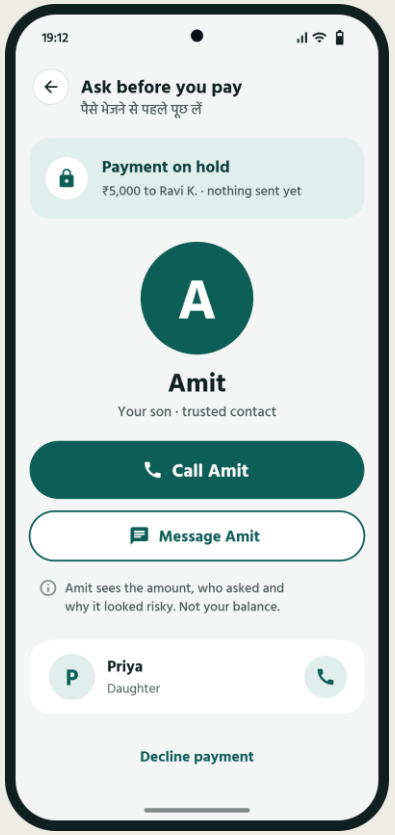
Screen 2 names the caller's trick: callers tell people to ignore this exact notice (P2).

Sample names and amounts.

Explain the scam in their language, out loud, then hand them a person.



3 · Why this looks like a scam



4 · Call family first

Listen in Hindi. P1: "make the screen speak out loud". P5 can't read English without her glasses.

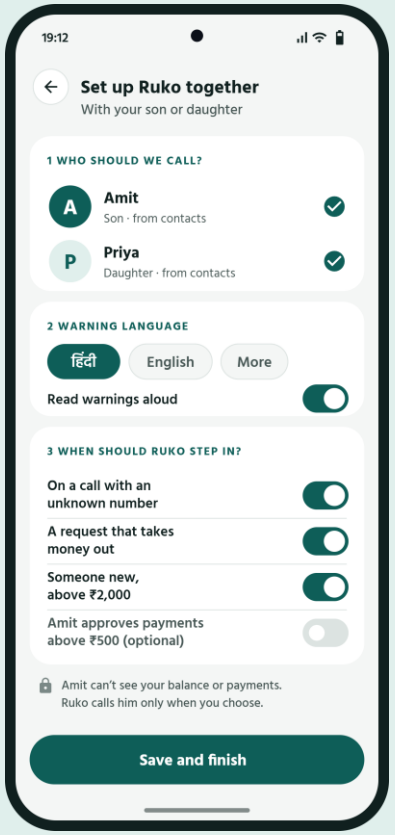
Three plain reasons, each with an icon and words, never colour alone.

A named person, not "contact support". Initials here, a photo in the real app (P5).

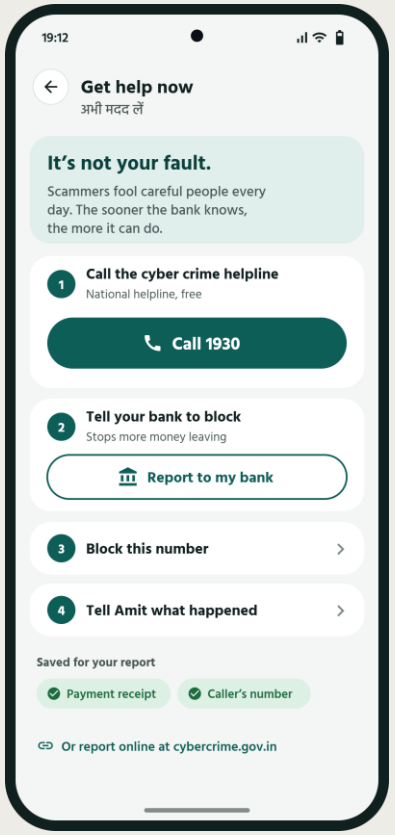
The payment waits; nothing is sent while they call. P3 wants "the exact rescue button".

Sample names and amounts.

Set it up together with family. After a scam: calm steps, and no blame.



5 · Trusted contact setup



6 · After a scam

Done together: family set up the payment app for 4 of 6 already.

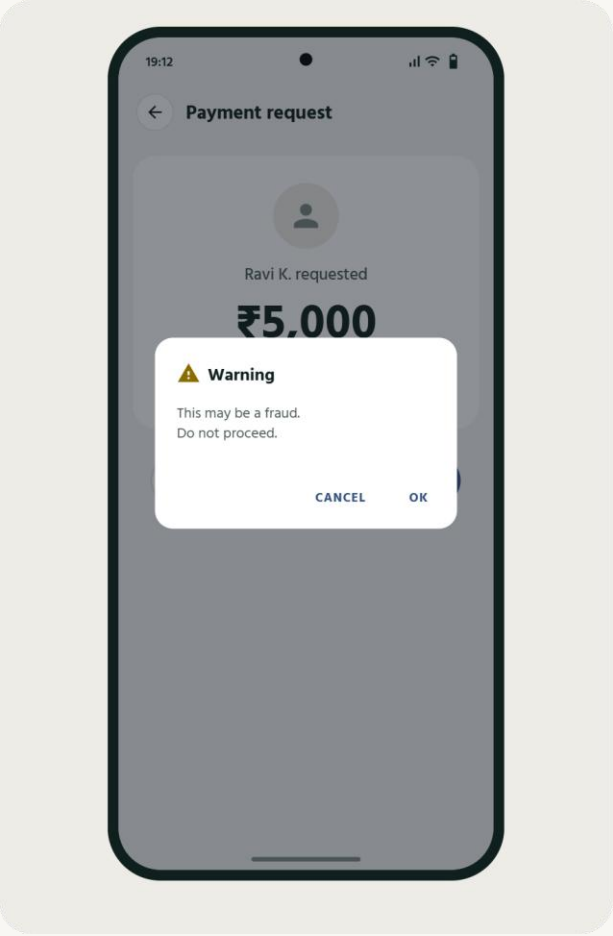
Checks fire on risk. Approving every payment over ₹500 is opt-in: P3 and P5 want it, P2 would hate it.

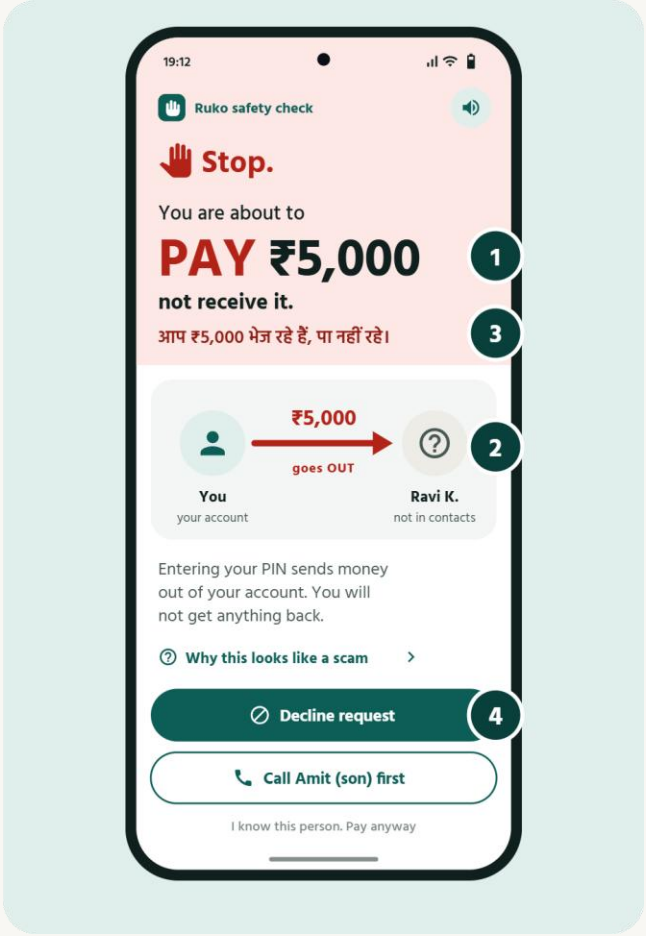
"It's not your fault" comes first. P4's bank told him "you gave the OTP yourself".

1930, then the bank, then family: the steps P4's daughter took him through.

Sample names and amounts.

Research turned a pop-up people tap past into a stop they read.





1. **The money and its direction come first**

   "Number 2 tells me the exact rupee amount going out." (P1)

2. **An arrow, not a word like "proceed"**

   2 of 6 stumbled on "proceed" (P1, P3).

3. **Their language, and spoken aloud**

   Asked for by P1 and P5.

4. **One safe main button, and a person**

   The generic warning "just scares you without telling you what to do next." (P5)

A warning earns belief when it explains why, names the cost, offers a person, and rarely cries wolf.

Explain why

"It doesn't tell me why it is fraud." (P4) Every stop links to plain reasons.

Name the real consequence

Money out, the exact amount. Warning 2: 6 of 6.

Offer a person

Family, by name, while the payment waits. Warning 3: 5 of 6.

Avoid false alarms

Context, not amount. "For small 20-50 rupees sabzi it will be irritating." (P1)

The risk: warning fatigue

If Ruko fires on the ₹65 ironing bill, it becomes one more "storage full" pop-up, and the real stop gets tapped away too. Every false alarm spends trust that the next warning needs.

Success is scams stopped, not warnings shown.

What I'd measure	How	Signal of success
Risky payments stopped	Share of warned payments declined or checked with family	High, and holding over time
False-alarm rate	Share of warnings on payments the person confirms as genuine	Low, and falling
Family call-through	Share of stop screens where the trusted person is called	Rising after setup
Losses after "pay anyway"	Reports to the bank or 1930 after a warned payment went ahead	Close to zero

Guardrail: never block people from their own money without a way forward.

Next: test the stop screen with people outside my family.

01

Usability test, 5 people aged 45+

Tasks: spot a “receive” request that pays out, call family from the stop, recover after a scam. Measure what they read and do.

02

Recruit beyond family

Other cities and languages, and people who have lost money, so the findings don’t rest on one kind household.

03

Check feasibility with a bank

The OTP-during-a-call and reported-account signals need partner data. Confirm before promising them.

What I learned

Designing for people unlike me meant borrowing their words and their trust. The best copy in this deck is “paise kat jayenge”, and the best button is a son’s name.

Thank you