

1 Motivation

- **Deepfake fraud** introduces new challenges to traditional anti-fraud strategies.
- **Victim experiences** with deepfake frauds remain understudied.

2 Research Questions

- **RQ1:** What types of deepfake or AI-enabled scams do people encounter, and how do they understand or interpret them?
- **RQ2:** How do individuals recognize or detect deepfake fraud in real-world situations?
- **RQ3:** What psychological, or financial impacts do victims experience?
- **RQ4:** How do victims respond to and report deepfake fraud, and what barriers do they face?

3 Methodology

- **Screening survey** to identify relevant scams experienced on social media, in video calls
- Follow-up interviews
- **7 interview** participants from 336 survey respondents.

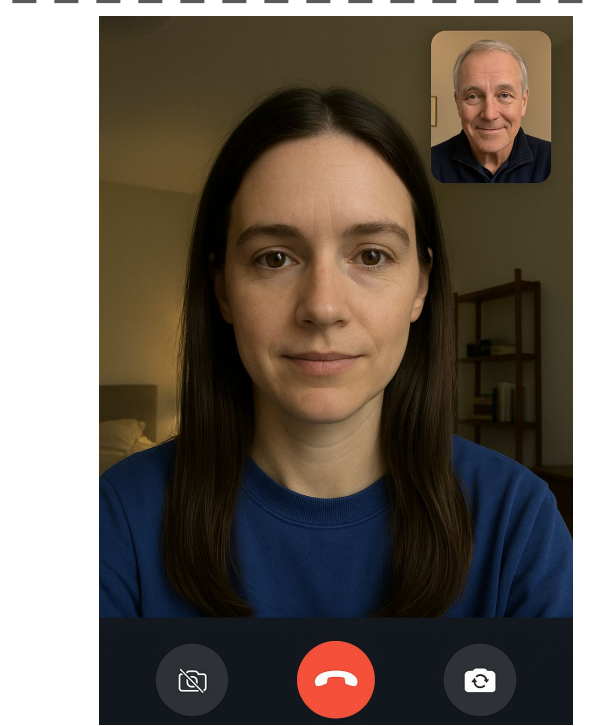
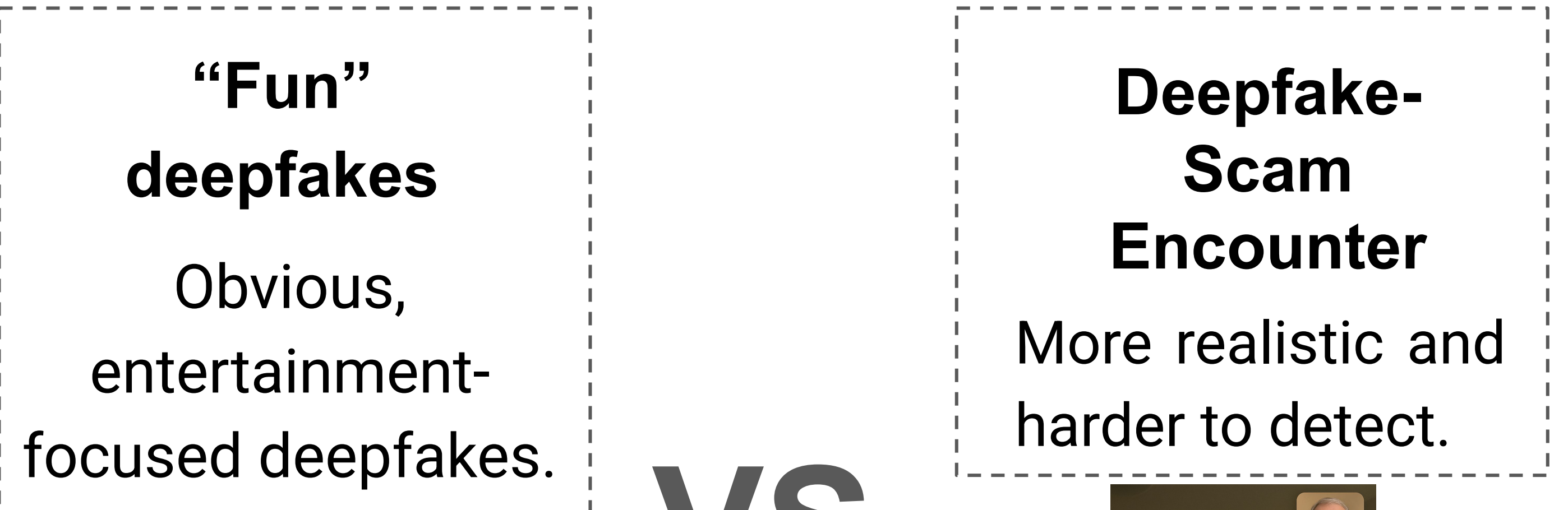
Interview Structure



4 Key Findings

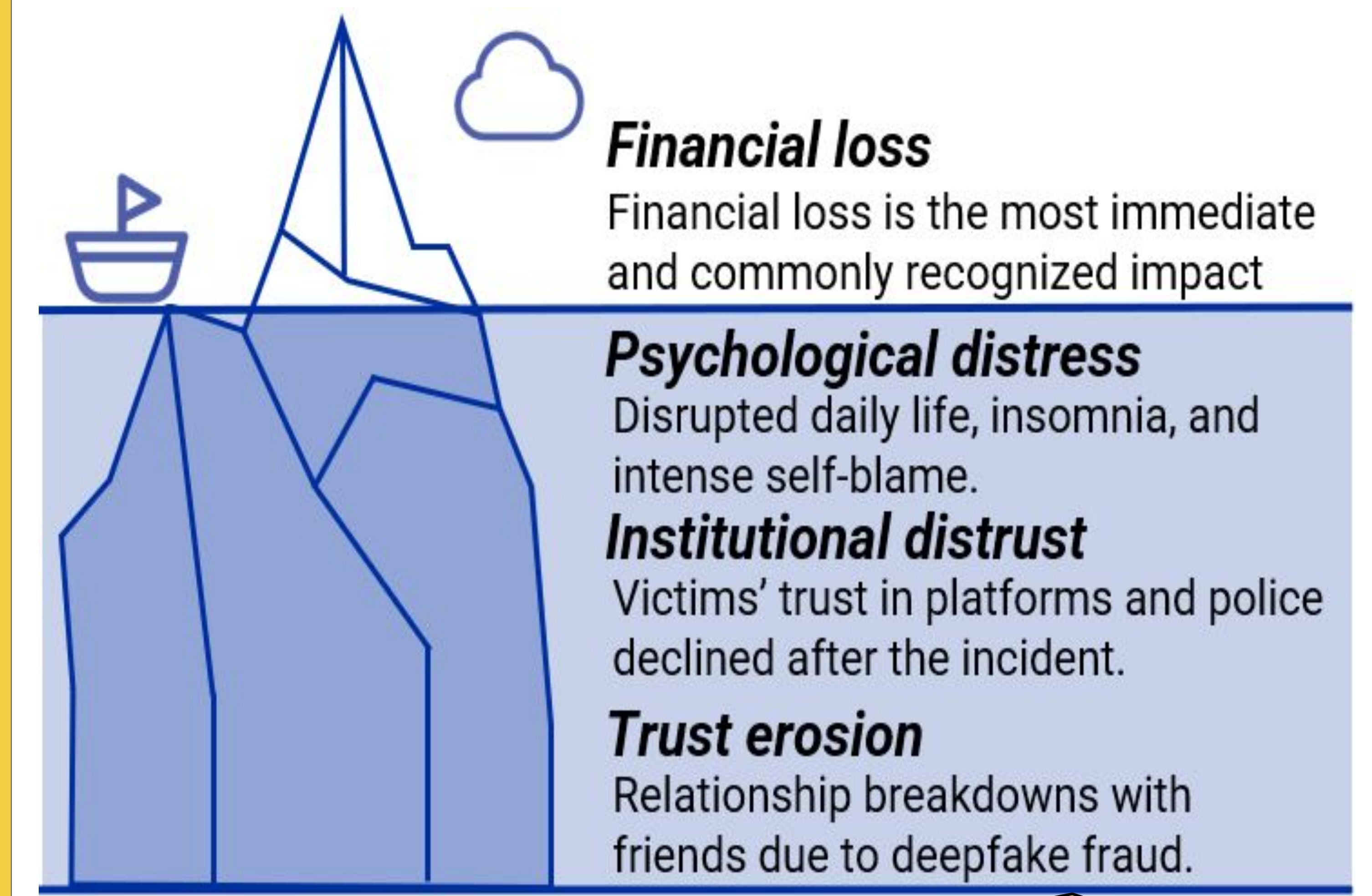
Detection Challenges

Mismatch in Mental Model of Deepfakes



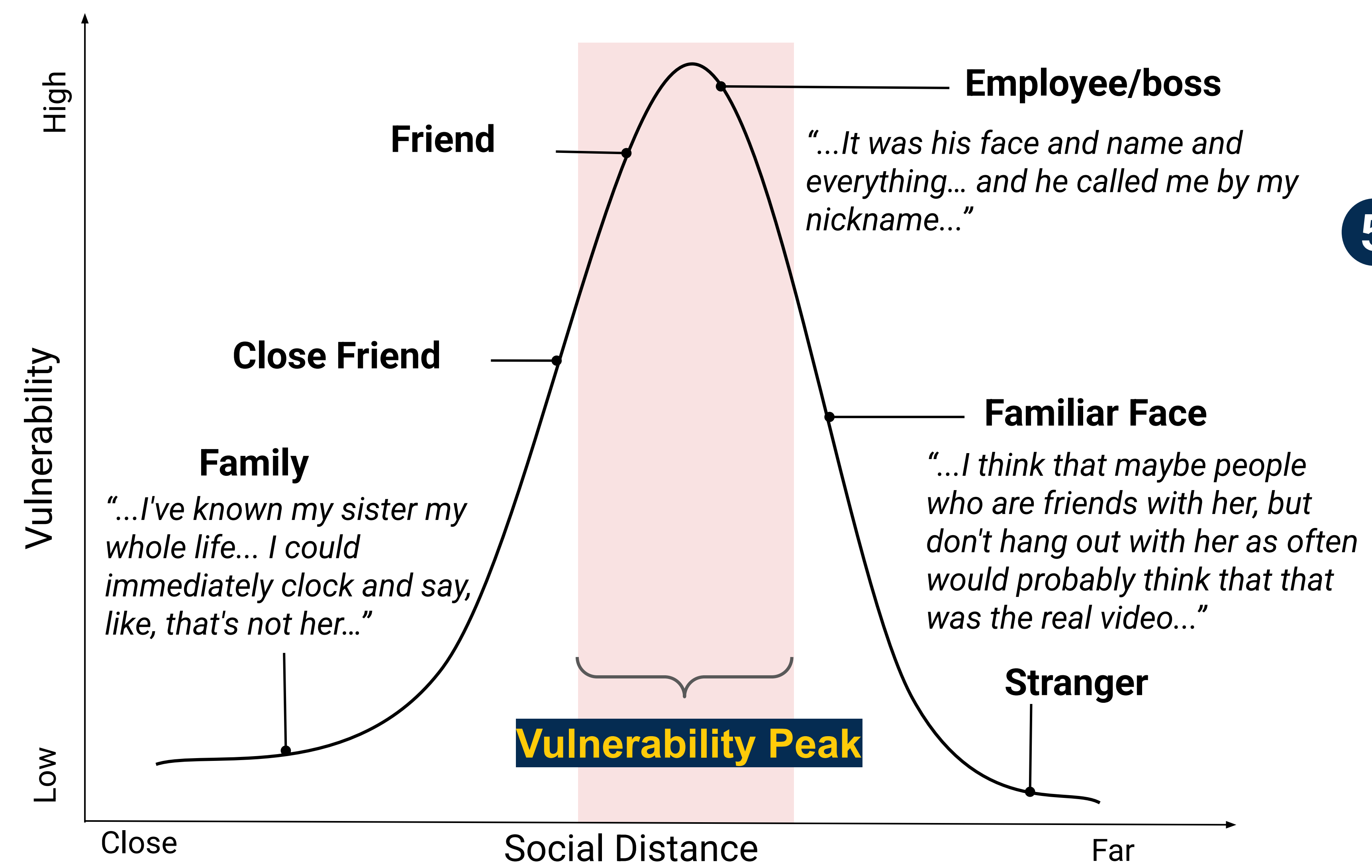
Result: Overestimate their ability to detect fraud.

Damage & Impact



“My friend told me that the person in the video call wasn't her. But thinking back, I was very familiar with her facial expressions. She is deceiving me!”

Vulnerability Peak



5 Takeaways

- Participants hold **mismatched mental models** of deepfake fraud, shaped by the mismatch between what they see and what they know.
- Frauds involving **moderately familiar** individuals are especially deceptive.
- **Hypervigilance in digital communication** and **broken trust** are severe consequences of deepfake fraud.
- Victims report **low confidence** in police and platform responses, highlighting gaps in institutional support.