.Cleafy

How NFC relay malware is breaking contactless payments and what banks must do now

Executive summary

Banks trust the tap. Attackers exploit that trust.

With NFC relay tools like SuperCardX, fraudsters are turning contactless into a remote attack vector, bypassing traditional defences without ever cloning a card, stealing credentials, or triggering transaction red flags.

There's no breach. No brute force.
No anomalies in the moment of payment.

Just real cryptographic data, silently forwarded across miles, and accepted without question.

Cleafy catches these threats before money moves.

Not by reacting faster, but by seeing earlier. Our session intelligence surfaces signals and patterns that traditional tools overlook, providing pre-crime visibility into fraud campaigns like SuperCardX.

The threat is already live and growing

£1.17B

UK fraud losses in 2024 — up 12% YoY

(Reuters, UK Finance)

SuperCardX is live, enabling cardless cashouts via infected Android phones

(Cleafy Labs, Cyware)

Relay fraud campaigns are spreading, with confirmed activity in Russia and early signs in the EU

(Risky Business Bulletin)

3.6×

Mobile malware exploded in one year

(SecureList)

What's lurking in the tap

Discovered by **Cleafy Labs**, SuperCardX is part of a growing class of lightweight Android malware, delivered through **Malware-as-a-Service (MaaS)** by Chinese-speaking threat actors.

Its capabilities reveal how much trust the system places in the tap:

- Hijacks a phone's NFC module for remote payments
- Requires minimal permissions - no overlays, no SMS access
- Evades AV, runtime checks, and fraud detection systems
- Spreads via smishing and sideloaded apps
- Enables cashouts from infected phones without user awareness

SuperCardX isn't just malware, it's a **test of blind trust**. The goal is to blend in, appear harmless, and act just enough to be dangerous. And today's defences are still passing it.

Cleafy didn't just detect SuperCardX after the fact. **We saw it before it activated**. Because we don't rely on malware to behave badly. We watch the signals that **precede** the fraud.

The new attack pattern: Real crypto, fake proximity

Here's how modern relay attacks work:

1. **A real tap happens** from a phone or card
2. **A relay device intercepts** the cryptographic data or malware like SuperCardX
3. **That data is forwarded** to a remote terminal
4. **The system sees a valid tap**, cryptographically perfect
5. **The payment is processed**, but neither the card nor the customer are present

This bypasses the basic assumption of contactless: **that the tap = the user is physically there.**

That assumption no longer holds.

Why traditional fraud tools miss it

Anti-fraud stacks typically operate post-transaction:

Traditional model	Relay reality
Transaction scoring	The tap is valid
Behavioural analysis	No anomalies at time of payment
Device fingerprinting	Device appears legitimate
Real-time risk checks	Data arrives cleanly

By the time the transaction reaches the fraud engine, it's already too late.

The attack has already succeeded.

Even digital wallets aren't immune

Digital wallets (Apple Pay, Google Pay, etc.) use secure elements to protect cryptographic keys. But SuperCardX doesn't need to break those keys, it just **relays** the data they produce.

It's like using someone's hotel key from across the city: The door unlocks because the key is valid, but the guest isn't anywhere near the hotel.

It's not an app hack. It's not a crypto break.

It's a **relay of trust**, and the system still believes it.

Why Cleafy caught it first

Cleafy doesn't wait for transactions. We observe **what happens before fraud has a chance to hide**.

While others monitor isolated events, we analyse entire sessions, from app open to transaction, across all behaviours and touchpoints:

- Which apps trigger NFC requests
- Session-level anomalies during login
- Subtle shifts in user behaviour mid-session
- Device overlap across multiple user journeys

Our **Mobile SDK** flags suspicious NFC activity the moment a session begins, giving fraud teams minutes or even days to act before any funds are at risk.

Traditional Tools	Cleafy FxDR Platform
Post-transaction scoring	Pre-session intelligence
Individual device view	Cross-session correlation
Anomaly detection	Narrative-based understanding
Alerts with context gaps	Actionable, explainable insights

Cleafy's **Mobile SDK** flags suspicious NFC activity the moment the banking session begins, giving fraud teams a window to act **before** damage is done.

What this means for banks

Contactless was built on the assumption of presence.

Relay attacks prove that this assumption is broken.

And that has consequences.

- For how we model risk
- For how we integrate fraud and cyber
- For how trust is verified or exploited

Cleafy provides the observability banks need to rebuild that trust:

- Detect session anomalies before any transaction
- Identify malware and fraud infrastructure early
- Neutralise in-session threats without disrupting UX
- Move from reactive alerts to proactive defence

What's at stake

This isn't a cryptographic flaw. It's a **systemic trust failure.**

One that turns digital banking into a battle-ground, not just for fraud teams, but for CISOs, CTOs, and COOs who now face questions about infrastructure-level risk.

Because once trust is broken at the point of tap, **it ripples outward** through channels, customer relationships, and brand perception.

Cleafy saw SuperCardX not because it behaved badly, but because **we saw the full story before it unfolded.**

We don’t trust the tap.
We trust what we see.

Let others score transactions.
Let others monitor red flags.

We monitor intent.
We decode behaviour.
We detect fraud before it becomes loss.

We are Cleafy. And this is what we’re built for.

Want to see what’s hiding in your sessions?

From NFC threats to zero-day fraud:
Cleafy helps you see what other miss, long before money moves.

Get in touch to learn more.

Learn more today

To learn more about how we can help you
> **Visit cleafy.com**
> **Email us at info@cleafy.com**

Trusted by leading European
and LATAM banks, boasting a 4.2 score
on Gartner Peer Reviews.

Gartner peerinsights™

Cleafy