KNOW THIS FACT: Why EasyBuy can’t hack your phonebook and blackmail your uncle over a ₦5,000 loan

LEGAL EYES

Why EasyBuy can’t hack your phonebook and blackmail your uncle over a ₦5,000 loan

The text message lands at 11:42 p.m.

“Tell Mrs. Grace Adebayo her son Tunde (0803* ****) is a FRAUDSTER. His ₦4,850 EasyBuy loan is 6 days overdue. We will paste his naked photo on Facebook. You are his guarantor PAY NOW or face court.”**

If this or anything like it has flashed across your WhatsApp, relax. Nigerian law is already wearing brass knuckles on your behalf. Below is a quick, plain-English audit of what the practice actually violates, the real-life implications, and the legal weapons you can fire back with.

1. What EasyBuy (and its cousins) are doing

Silent app-permission grab: When you install the app you click “allow” to contacts, camera, location, etc.

Back-end scraping: Phone numbers of everyone you know are copied to their server—without consent of those third parties.

Auto-generated threat SMS/WhatsApp: Round-the-clock robocalls to you, your boss, your pastor, your ex.

2. The Nigerian laws they break

Law / Regulation	What it forbids	Section / Article
Cybercrimes Act, 2015	Unauthorised access to a computer (your phone); using data to blackmail	S. 6, S. 17
Nigeria Data Protection Act, 2023	Processing personal data without explicit consent; sharing with third parties	Part V & VI
CBN Consumer Protection Framework	Calling contacts unless they are guarantors; harassment, threats, night calls (8 pm–8 am)	Para 5.5.7 A–C
FCCPC Digital Lending Guidelines, 2022	Must register with the Commission; must disclose purpose of data; no intimidation	Clause 8-10
Criminal Code (Southern States)	Criminal defamation, threat to life, blackmail	Ch. C38, LFN 2004

Sharing your contact list after default is NOT covered by the tiny window that allows lenders to phone guarantors—because 99 % of your contacts never guaranteed anything.

3. Real-world damage

- Job loss: Employers receive threat messages, assume fraud, withdraw offer letters.
- Mental health: Victims report panic attacks, suicidal ideation.
- Community shame: Public WhatsApp groups circulate defamatory posters.
- Financial exclusion: Genuine fintechs blacklist victims over false “fraudster” tags.

4. Legal solutions: Fight back in 5 moves

Stop	Action	Where / How
Document	Screenshot every threatening message, call log, voice note.	Save to Google Drive + email yourself (time-stamp evidence).
Complain	File joint petition to: • NITDA (data breach) – petro@nitda.gov.ng • FCCPC (harassment) – consumer@fccpc.gov.ng • CBN (if lender is CBN-licensed) – cpd@cbn.gov.ng	Part V &Attach evidence, demand investigation and sanction. VI
Police & EFCC	If threat contains death wish, blackmail, extortion.	Write to Cyber-Crime Unit, Force HQ, Abuja or nearest EFCC zonal office. Attach evidence.
Sue For Damages	Engage a lawyer; file Fundamental Rights suit at Federal High Court.	Reliefs: ₦10m–₦50m damages, public apology, perpetual injunction. Use FREP Rules 2009.
App Take-Down	Report app to Google Play / Apple App Store for policy violation.	Include NITDA or FCCPC acknowledgement letter as proof.

5. Precedents you can ride on

- SOKOLOAN – NITDA slammed ₦10m fine for invasive messages to contacts.
- Confidence Staveley v Access Bank – Court awarded damages for unauthorised data sharing.
- Paradigm Initiative v NIMC – First case where NDPR breach was recognised as breach of privacy right.

6. Quick checklist before you borrow next time

✅ **Read permissions** – Deny access to contacts, photos, location if unrelated to the loan.

✅ **Check license** – Only download FCCPC-approved apps (list at fccpc.gov.ng/approved-lenders).

✅ **No guarantor?** – They MUST NOT call your contacts.

✅ **Record calls** – Legal in Nigeria if you are a party to the conversation.

✅ **Withdraw consent** – Email them: "I withdraw consent to process my data; delete within 7 days." (They must comply – NDPR s. 3.1(9)).

Bottom line

Threatening your friends or defaming you because of a ₦5,000 loan is not debt recovery—it is data theft, defamation, extortion and cyber-stalking, all rolled into one. Nigerian law is on your side; regulators are already fining and delisting rogue apps. Document, report, sue—and let the sharks choke on their own poison.