FIDBACC INVOICE

A 12-PAGE REPORT FOR SMES · NDPA 2023 EDITION

The Hidden Cost of "Free" Invoice Generators

What your free tool's terms of service don't tell you about your customer list — and why, under Nigeria's Data Protection Act 2023, it's *your* problem when it leaks.

Victor Omolayo · Founder, Fidbacc Invoice
invoice.fidbacc.com

2026

CONTENTS

What this report covers

WHY WE WROTE THIS

If you've ever sent an invoice through a "free" web tool, the customer's name, phone, and address probably left your control the moment you uploaded them. Most vendors don't know it — until their best customer starts getting Bitcoin spam and asks *"why did you give my number out?"*

This report is the answer to that conversation, before it happens.

PART ONE

The invoice you sent last Tuesday

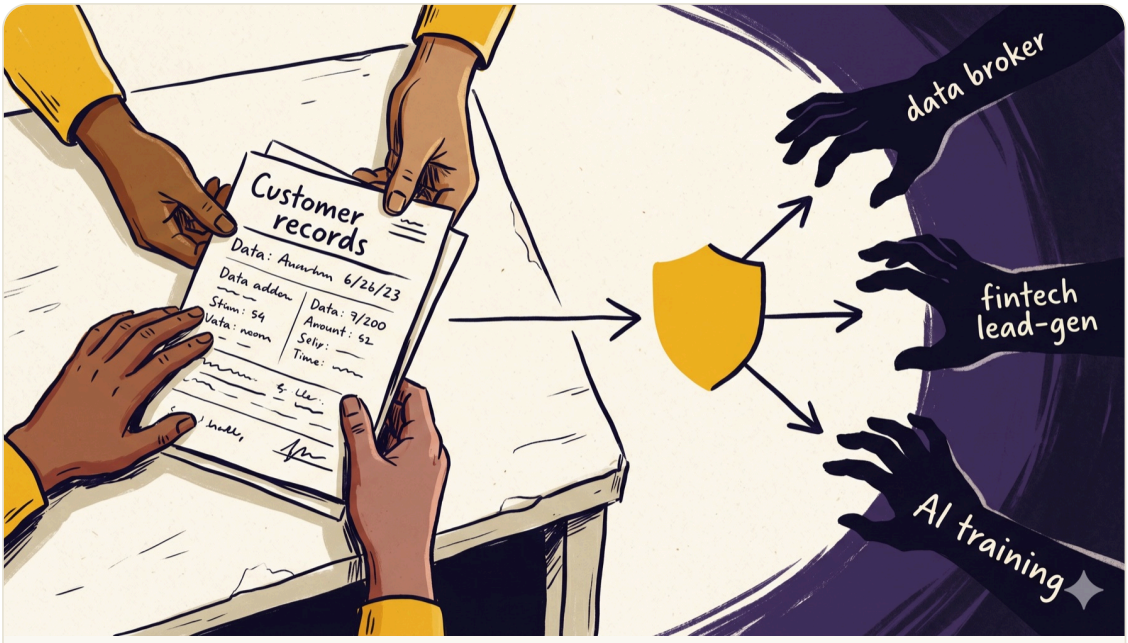
Last Tuesday, you typed a customer's name, phone, address, and order details into a free invoice generator. You hit download. You sent the PDF on WhatsApp. You moved on with your day.

Two weeks later, that customer calls you. They're irritated. *"I'm getting Bitcoin texts and crypto loan offers since I bought from you. Did you give them my number?"*

You didn't. You'd never. But somewhere between your keyboard and the customer's phone, that data left a trail. And the trail does not lead back to a hacker. It leads back to the **"by clicking download you agree..."** checkbox you didn't read on a Tuesday afternoon eight months ago.

> *The free tool didn't get hacked. It worked exactly as designed. Your customer's contact details were the price you paid for a "free" PDF.*

This is not a horror story. It's a business model. And under Nigeria's Data Protection Act 2023, when the leak happens, the regulator looks at **you** first — not the tool you used.



Spot 01 · The invisible exit

PART TWO

The business model of "free"

Hosting a web app costs money. Servers, engineers, support staff, payment processors. Nobody runs a free invoice generator out of charity.

So when a tool says **"free forever, no credit card,"** it has to make money somewhere. There are exactly four places it can come from:

- ✓ **Upsells** — most users never pay; the few who do subsidise everyone.
- ✓ **Ads** — banners, popups, "sponsored partners".
- ✓ **Affiliate fees** — embedded payment links that take a cut.
- ✓ **Your data** — the customer records you upload, packaged and sold.

The first three are visible. You can see the upgrade prompt. You can see the banner. You notice when the "Pay Now" button funnels through Stripe.

The fourth one — your data — is invisible. It's hidden in the Terms of Service, written in a font small enough that nobody reads it. And it is, by far, the most lucrative of the four.

What the TOS clause actually says

Read carefully. This is the kind of language you'll find on a "free" invoice generator's Terms of Service page. Verbatim patterns collected from active free tools (we've kept the patterns and dropped the names — the point is to teach you what to read for, not which vendor to avoid this week):

PATTERN A — THE BROAD LICENCE

"You hereby grant us a non-exclusive, worldwide, royalty-free, sublicensable licence to use, reproduce, modify, distribute, and display the data you upload, including for product improvement, analytics, and partnerships with third parties."

PATTERN B — THE "ANONYMISED" LOOPHOLE

"We may share aggregated or anonymised data derived from your usage with our commercial partners. Aggregated data does not identify any individual."

In practice, "anonymised" customer records can often be re-identified using two or three of: phone number, address, transaction amount.

PATTERN C — THE AI TRAINING CARVE-OUT

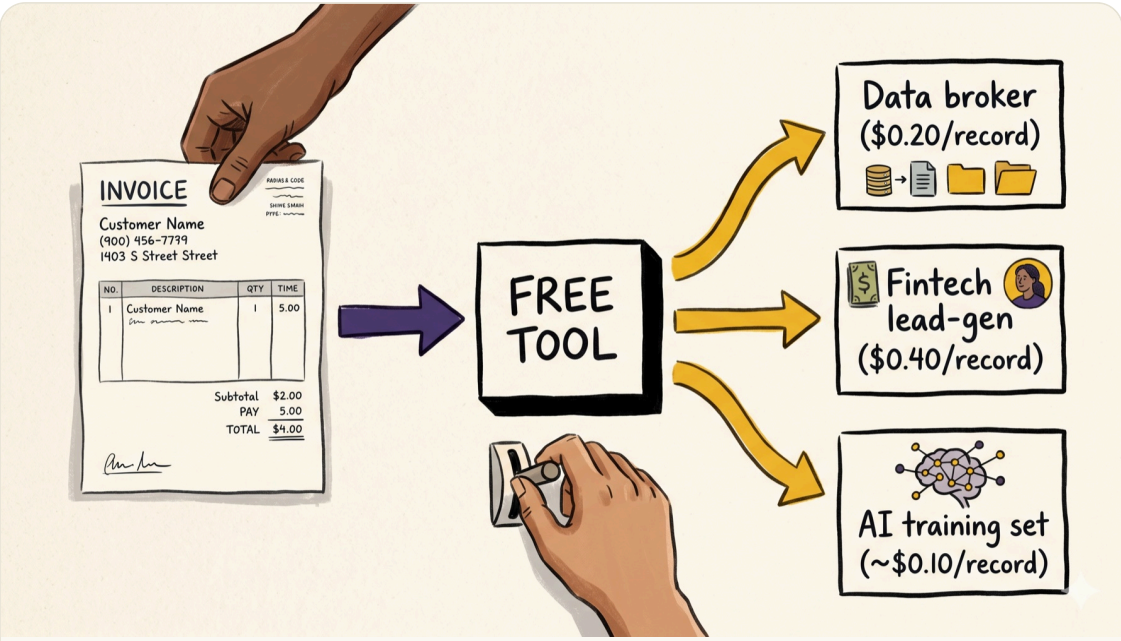
"We may use uploaded content, including invoice metadata, to train, test, and improve our machine learning models and those of our research partners."

None of these clauses are illegal. Most are contractually enforceable. The only thing wrong with them is that the user — you — never read them. And by clicking *"download invoice"*, you signed.

PART THREE

The data broker pipeline

Once a free tool has the right to "share aggregated data with partners," here's where the data goes.



Spot 02 · How the pipeline works

Step 1: collection

You enter customer name, phone, email, address, item, amount. The tool stores it permanently — even if you "delete" the invoice from the dashboard. (Most TOSs allow soft-delete only.)

Step 2: aggregation

Records from thousands of vendors are merged into a single dataset. Names paired with phone numbers paired with purchase patterns paired with addresses. **This is the product.**

Step 3: resale

Aggregated records are sold to data brokers. The 2014 FTC report on the data-broker industry (still the most comprehensive public study) documented per-record pricing in a wide range:

Buyer type	Typical use	Per-record price
Generic data broker	Reseller marketplace	$0.10 – $0.20
Fintech lead-gen	Loan-offer SMS targeting	$0.30 – $0.50
Telco lead-gen	Cross-sell campaigns	$0.15 – $0.25
AI training partner	NLP / OCR data sets	$0.05 – $0.15

That looks small until you multiply. A free tool with **500,000 active users averaging 8 customer records each** = 4 million records. Sold once at $0.20 = $800,000. Sold across 5 buyer categories with different use cases = several times that. Annual.

Step 4: the spam your customer receives

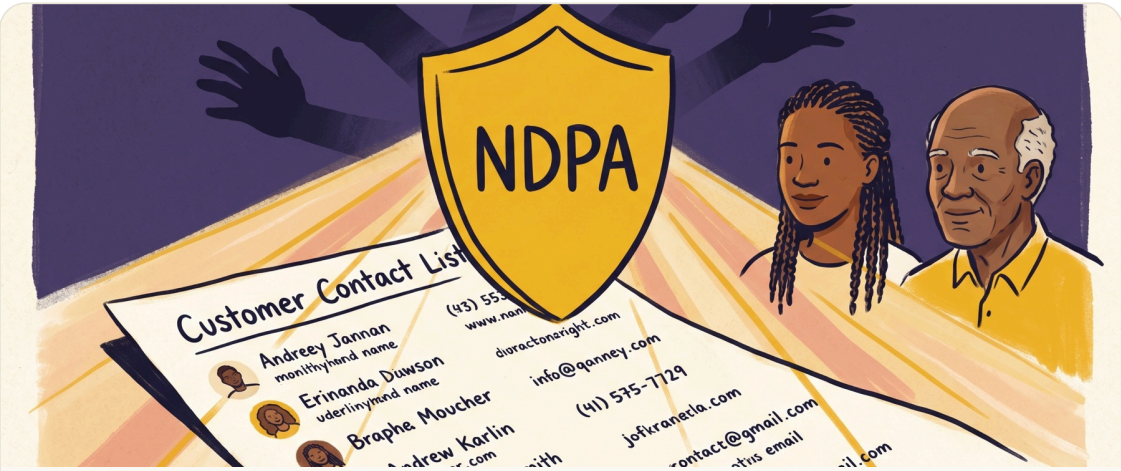
Two weeks after you sent the invoice, your customer's number lands on a fintech outbound list. They get an unsolicited "we noticed you recently made a purchase — would you like a loan?" SMS. They blame the most recent business they bought from. They blame you.

> *The data broker is invisible. The customer's anger is not. The trust you spent six months building can disappear over a single Bitcoin spam text.*

PART FOUR

Why it's *your* problem — NDPA 2023

Nigeria passed the Nigeria Data Protection Act in June 2023. It is the first comprehensive data-protection law in Nigerian history. And it puts the legal liability for customer data breaches on the small business owner — not on the tool they used.



Spot 03 · NDPA 2023 in plain English

You are a "data controller"

Under **NDPA 2023, Section 30**, anyone who "determines the purposes for and the manner in which personal data is processed" is a **data controller**. That means: if you decide which customer to invoice, what fields to capture, and how the data is used in your business — congratulations, you are a regulated entity.

You don't have to be a bank. You don't have to be a corporation. You don't have to be making ₦1 billion. **If you collect customer information, you are a controller, full stop.**

What controllers are obligated to do

Read **NDPA 2023 §24-30** in full if you have time. The condensed version:

- ✓ You must collect personal data only with a **lawful basis** (usually consent, or contractual necessity).
- ✓ You must process the data **only for the purposes you collected it for.**
- ✓ You must **protect** the data with reasonable technical and organisational measures.
- ✓ You must allow customers to **request a copy** of their data, request correction, and request deletion.
- ✓ You are **liable** for breaches caused by the processors you choose to use — including the free invoice tool you uploaded data to.

The penalty structure

Under **NDPA 2023 §48**, the Nigeria Data Protection Commission can impose enforcement action against controllers and processors. Penalties for material violations can be substantial — the most serious cases can attract significant percentage-of-turnover fines, with smaller fixed-amount penalties available to the Commission for less severe violations.

> *Translation: when your customer's data leaks from the free tool you used, the regulator does not call the free tool. The regulator calls **you**.*

This page summarises the author's reading of NDPA 2023 in plain English. It is **not legal advice.** Consult a qualified Nigerian privacy lawyer before relying on these statements for compliance decisions. The Nigeria Data Protection Commission publishes updated guidance regularly; verify current penalty schedules at ndpc.gov.ng.

PART FIVE

The global picture

If you operate in Ghana, Kenya, or sell to diaspora customers in the EU or UK — the same pattern applies, with different statutes attached.

Region	Statute	What it covers (in plain English)
Nigeria	NDPA 2023 + GAID 2025	You are a data controller the moment you collect customer info. You are liable for processor breaches.
Ghana	Data Protection Act 2012 (Act 843)	Similar controller / processor framework. Mandatory registration with the Data Protection Commission for businesses that process certain data categories.
Kenya	Data Protection Act 2019	Mirrors GDPR-style obligations. ODPC has been active in enforcement since 2022.
EU / UK	GDPR + UK GDPR	If you have a single customer in the EU or UK, you are likely subject to GDPR. Penalties are well-publicised: up to 4% of global turnover.

The point is not to memorise the statutes. The point is: **"the free tool's TOS made me do it"** is not a defence in any of these jurisdictions. The vendor who chose the tool is on the hook.

This is true even if your business is small. It's true even if you didn't read the TOS. It's true even if the data went to a partner of a partner of a partner.

PART SIX

What to look for in any tool's TOS

Ten minutes. Ctrl+F. Five terms. If any of them appear in the tool's Terms of Service or Privacy Policy, it's time to look at alternatives.

- ✓ **"Non-exclusive licence"** — over user-uploaded content. Means they can use it for anything they want.
- ✓ **"Aggregated"** or **"anonymised"** data sharing — the loophole that allows resale to brokers.
- ✓ **"Partnerships"** with third parties — the receiving end of that resale.
- ✓ **"Analytics"** and **"product improvement"** — broad enough to cover almost any data use.
- ✓ **"Train AI"** or **"machine learning"** — your customer data may be in the next foundation model.

10-MINUTE AUDIT CHECKLIST

1. Open the tool's TOS and Privacy Policy in a browser tab.
2. Use Ctrl+F (or ⌘+F) to search each of the five terms above.
3. If any clause grants the tool rights over your *uploaded data* (not just usage logs), screenshot it and date the screenshot.
4. Check whether you can export your customer list as CSV. If not — red flag.
5. Check the right-to-deletion policy. "Soft delete" is not deletion.

PART SEVEN

What Fidbacc does differently

Our terms of service do not include the patterns above. Specifically:

- ✓ **No non-exclusive licence over your customer data.** What you upload remains yours.
- ✓ **No "aggregated" loophole.** We do not aggregate or anonymise customer records for resale.
- ✓ **No data broker partnerships.** We do not have data-broker partners, full stop.
- ✓ **No customer data used for AI training.** Voice-to-invoice runs through Gemini, but transcripts are not retained beyond invoice generation and are never used to train shared models.
- ✓ **Real export.** Every Pro user can export the full customer list as CSV at any time.
- ✓ **Real deletion.** When you delete a customer, the record is hard-deleted from active databases within 30 days, including from backups.

HOW WE MAKE MONEY

Fidbacc Pro is **₦1,750/month.** That is the entire business model. The 5,000+ free users are subsidised by the people who upgrade because we earn the upgrade. We do not need — and do not want — to monetise customer data to keep the lights on.

> *If a free tool can't tell you exactly how it makes money, you are paying. You just don't know with what.*

PART EIGHT

What to do this week

- **Audit your current invoicing tool's TOS** using the 5-term checklist on the previous page. 10 minutes.
- **Export your customer data** from the tool. Most allow this; some do not. Inability to export = red flag.
- **If TOS contains the patterns** — open a new tool (Fidbacc, or any tool that passes the checklist), import your customers, and delete your old account.
- **Tell your customers what changed.** A short WhatsApp note: "I just moved my invoicing to a tool that doesn't share data. Same service, no spam." Builds trust on its own.

A closing letter

I built Fidbacc because I watched a vendor I cared about lose two long-term customers over Bitcoin spam they had nothing to do with. The customers blamed her. She had no defence — she didn't know where the leak came from, because the leak came from a tool whose TOS she'd never read.

The point of this report is not to make you panic. It's to make you **read the TOS once** — and then make a decision you can actually defend.

If Fidbacc is part of that decision, we'd love to have you. If it's a different tool, we still want you to be safe. The harm is real.

— **Victor Omolayo**
Founder, Fidbacc Invoice
+1 (203) 646-1089 · invoice.fidbacc.com

> This report describes the author's reading of NDPA 2023, GDPR, and related statutes in plain English. It is **not legal advice.** Consult a qualified Nigerian privacy lawyer for compliance decisions specific to your business.

FIDBACC INVOICE

Your customer data stays yours.

Voice-to-invoice on WhatsApp. FIRS-compliant. No data resale, ever — written into our TOS.

invoice.fidbacc.com/your-data-is-yours

WhatsApp: +1 (203) 646-1089