

PRIVACY POLICY

1 ABOUT FCMB

First City Monument Bank (FCMB) Limited is a member of FCMB Group Plc, which is one of the leading financial services institutions in Nigeria that are market leaders in their respective segments. Having successfully transformed to a retail and commercial banking-led group, FCMB expects to continue to distinguish itself by delivering exceptional services, while enhancing the growth and achievement of the personal and business aspirations of our customers.

2 INTRODUCTION

FCMB conducts business in a responsible and sustainable manner and ensures customer information are securely collected, processed, and stored based on business requirements. In furtherance to this and compliance with industry regulations, FCMB has made appropriate documentation, which includes a privacy policy. FCMB therefore provides notice about this policy, applicable procedures and identifies the purposes for which personal information is collected, used, processed, disclosed, retained, and disposed.

Throughout this Privacy Policy, we use the term "personal information or data" to describe information that can be associated with a specific person and can be used to identify that person. We do not consider personal information to include information that has been made anonymous so that it does not identify a specific user.

This policy also reflects our commitment to compliance with the Nigeria Data Protection Act (NDPA). It ensures data subjects' rights are respected, and personal data is processed fairly, lawfully, and transparently.

FCMB ensures equal access to privacy information for individuals with disabilities and low literacy levels. We offer simplified versions of this policy as well as alternative communication formats—including audio, large print, and screen-reader compatible documents. Requests for accessible formats can be directed to the Data Protection Officer.

3. Information we may collect about you.

3.1 Your Personal Information

At FCMB, we strive to meet your needs and provide you with exceptional services. While consuming our services through various channels, such as forms, phone calls, correspondence, service point interfaces, and other available channels, we collect information that you provide to us.

This information may include, but is not limited to, contact data, log/Technical information, Financial Data, Marketing and Communications Data, identity verification details (this include

Personally Identifiable Information (PII), otherwise known as Personal Information or Personal Data, which includes email address, phone number, contact address, limited financial information, location data, device data etc.) and documents, services consumed or desired, mode of consumption, preferences, location, general events, and instructions and transactions relating to the services.

In the process of using our services, our facial recognition and biometric fingerprint devices (such as ATMs, mobile applications etc.) and CCTV cameras, in operation may capture your personal / sensitive data. Before the deployment of new solutions for our operations, consideration would be made on the impact of emerging technology /software / project on our data subjects in our DPIA.

Legal basis for processing:

- I. Your Consent: Where you agree to us collecting your Personal Information by using our Services.
- II. We have a contractual obligation: Without your Personal Information, we cannot provide our Services to you.
- III. We have a legal obligation: To ensure we are fully compliant with all applicable financial legislations such as Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) Laws, we must collect and store your Personal Information. We protect against fraud by checking your identity with your Personal Information.
- IV. Legitimate Interests: We may process your data to pursue our legitimate interests, such as preventing fraud, improving our services, or sending you personalized offers, provided these interests do not override your constitutional rights and freedoms.

While we may utilize data from third-party sources, all vendors and service partners that process personal data on behalf of FCMB are subject to legally binding Data Processing Agreements (DPAs). These agreements outline our expectations for privacy safeguards, processing limitations, and audit rights to ensure accountability and regulatory compliance.

Additionally, to better serve your needs, we may utilize information about you collected from third parties and service partners. It is important to note that these third-party sources are not under the control of FCMB, and we are not responsible for how they use the information.

In line with the NDPA mandates, FCMB conducts a legal basis assessment for all data processing operations and maintains a record of processing activities (RoPA) as required by law.

3.2 Usage and other information

In addition to the personal information described above, we may collect certain information about your use of our online services. For example, we may capture the IP address of the device you use to connect to the online service, the type of operating system and browser you use, and information about the site you came from, the parts of our online service you access, and the site you visit next. FCMB or our third-party partners may also use cookies, web beacons or other technologies to collect and store other information about your visit to, or use of, our online services. In addition, we may later associate the usage and other information we collect online with personal information about you.

3.3 FCMB Mobile

For the convenience of our FCMB customers, we provide access to our products and services through our mobile applications and mobile-optimized websites ("FCMB Mobile"). When you engage with us through FCMB Mobile, we may collect certain information to enhance your experience. This information may include unique device identifiers for your mobile device, screen resolution, device settings, location information, and analytical data regarding your mobile device usage. Please note that we may request your permission before collecting specific information, such as precise geo-location data, contact or image data, and other personally identifiable information through FCMB Mobile. Rest assured that any information collected is handled with the utmost care and in accordance with our privacy policy.

3.4 Additional sources of information

We may also collect information about you from additional online and offline sources including from co-branded partner sites or commercially available third-party sources, such as credit reporting agencies. We may combine this information with the personal and other information we have collected about you under this Privacy Policy.

3.5 Non-Personal Information

To achieve our goal of providing you with the best-in-class service, we may also collect, store, use, and transfer non-personal information or anonymized data such as statistical or demographic data. These may be collected or sourced during your visits to perform certain tasks such as grant you access to some parts of our website or conduct research on your behavior on our site to improve our services. We will not disclose your information to any person outside our organization except as described in this Privacy Policy.

4. How we use collected Information

FCMB may use or process the information discussed above in several ways, such as to:

- Manage your preferences.

- Create and manage any accounts or transactions you may have with us, verify your identity, provide our services, and respond to your inquiries.
- Process your applications and transactions (including authorization, clearing, chargebacks and other related dispute resolution activities).
- Protect against and prevent fraud, unauthorized transactions, claims and other liabilities as well as enhance the security of your account or our online services.
- Provide, administer and communicate with you about our products, services, offers, programs and promotions as well as those of our merchants and partners.
- Evaluate your interest in employment and contact you regarding possible employment with FCMB.
- Evaluate and improve our business, including developing new products and services.
- To target advertisements, newsletters, and service updates.
- As necessary to establish, exercise and defend legal rights.
- Perform analytics concerning your use of our online services, including your responses to our emails and the pages and advertisements you view.
- As may be required by applicable laws and regulations, including for compliance with Know Your Customers and risk assessment, Anti-Money Laundering, anti-corruption and sanctions screening requirements, or as requested by any judicial process, law enforcement or governmental agency having or claiming jurisdiction over FCMB or affiliates.
- To use data analytics to improve our website, products, or services, and user experiences.
- For other purposes for which we provide specific notice at the time you provide, or we collect your information.

During our operations, we collect and process various categories of personal data based on our relationship with individuals and entities. These categories include:

- Employee and Directors' Data: includes names, contact details, job titles, employment history, payroll information, and identification documents.
- Pre-Employment Medical Assessment Data: includes health assessments conducted for recruitment purposes, medical clearance reports, and related sensitive data.

- Recruitment Candidate Data: includes CVs, cover letters, contact information, academic and professional qualifications, references, and interview evaluations.
- Contract Staff Data: includes personal and professional details of contract workers engaged for short-term or outsourced roles.
- Customer Data: includes name, contact details, transaction history, identity verification data (e.g., BVN, NIN), and account-related information.
- Cardholder Data: includes cardholder name, card number (where applicable), and encrypted payment data, handled in accordance with PCI DSS standards.
- Website Visitor Data: includes IP address, browser type, usage patterns, cookies, and device metadata.
- Vendor and Third-Party Data: includes business contact details, tax and payment details, bank information, and due diligence documents.
- Voice Data: includes recorded voice calls for customer service, compliance, or training purposes.
- Webinar Attendee Data: includes names, email addresses, job titles, and engagement data collected during virtual events.
- Survey Respondent Data: includes feedback, demographic data, and opinions collected from individuals who participate in surveys.
- Interview Participant Data: includes consented audio/video recordings, transcripts, and responses during qualitative or quantitative interviews.
- Visitor Data: includes physical visitor logs, name, company, purpose of visit, and identification as required by our access protocols.
- CCTV Surveillance Data: includes video recordings captured on our premises for security and monitoring purposes.

We may also use data that we collect on an aggregate or anonymous basis (such that it does not identify any individual customers) for various business purposes, where permissible under applicable laws and regulations.

5. Data Privacy Impact Assessment

FCMB makes use of a privacy by design system and performs a periodic assessment of the risks to the rights and freedom of data subjects. This also includes the scope of processing activities,

the purpose and proportionality of processing, as well as security mechanisms that guarantee personal data protection.

For high-risk processing activities, FCMB implements appropriate residual risk evaluations post-Data Protection Impact Assessments (DPIAs). This ensures that any remaining risks to data subjects' rights and freedoms are clearly documented, and where necessary, mitigated or escalated to the Nigeria Data Protection Commission (NDPC).

We also ensure the continuous monitoring of identified risks and update DPIAs where there are changes in processing conditions, technology, or regulations.

6. Customer Data Protection Rights

Our customers have data protection rights and are entitled to the following:

- The right to access – Customers have the right to request copies of their personal data. FCMB may charge a fee for this service if it will require a substantial amount of resources to accomplish.
- The right to rectification – Customers has the right to request that FCMB corrects any information they believe and have proven to have been captured inaccurately. Customers also have the right to request FCMB to complete the information they believe is incomplete.
- The right to erasure – Customers has the right to request that FCMB erase their personal data, under certain conditions. These conditions are not limited to regulatory requirements, law enforcement agencies, or where such action may cause disruption to our system.
- The right to restrict processing – Customers have the right to request that FCMB restricts the processing of their personal data, under certain conditions. (as above)
- The right to object to processing – Customers have the right to object to Our Company's processing of your personal data, under certain conditions. (as above)
- The right to data portability – Customers have the right to request that FCMB transfer the data that we have collected to another organization, or directly to them, under certain conditions. (as above)
- The Right to Be Informed - Customers have the right to receive clear, concise, and accessible information about how their personal data is collected, used, shared, and stored.

- The Right to Object to Automated Decision-Making and Profiling - Customers have the right not to be subject to decisions made solely by automated means, including profiling, which significantly affects them (e.g., credit scoring, hiring decisions).
- The right to complain to Supervisory bodies - Customers have the right to lodge a complaint with the supervisory authority, the Nigeria Data Protection Commission (NDPC), if they believe FCMB has not processed their personal data in accordance with the NDPA. In case of infringement or breach of Data Subject rights, please contact (info@ndpc.gov.ng)

Customer requests shall be handled within 14 working days for standard cases and up to 28 working days for complex cases. FCMB will not charge fees unless requests are manifestly excessive or unfounded. Customers may contact FCMB by email, or phone listed below.

Email: dataprotection@fcmf.com and customerservice@fcmf.com

Phone number: 02012798800, 0700-3290000

7. The Use of Cookies and Similar Technologies

FCMB's websites use two types of cookies:

- Session cookies – These are temporary cookies that remain in your browser's cookie file only until you close your browser. They are automatically deleted once your session ends.
- Persistent cookies – These remain on your device for a longer period or until manually deleted. They help the website remember your preferences and improve your user experience.

Cookies do not access or read any files on your hard drive, gather personal information from your device, or identify you personally—unless you have logged into an authenticated (secure) section of the website.

Cookies cannot be used by anyone else with access to your device to obtain information about you. They do not compromise the security of your computer or device in any way.

FCMB does not use cookies to contact you for marketing purposes outside the website. However, cookies may be used to record pages you visit, particularly those related to FCMB products or services. This helps us understand user interests and improve the content and functionality of our website.

Most web browsers are configured to accept cookies by default. However, you can modify your browser settings to:

- Disable cookies entirely,
- Notify you when a website attempts to place a cookie,
- Or delete cookies already stored on your device.

Please note: If you disable session cookies, you may still browse unsecured areas of our website, but you might not be able to log in to secure (authenticated) sections.

Please visit <http://www.allaboutcookies.org/manage-cookies/> to discover how to disable and delete cookies.

8. Disclosures

8.1 Disclosures

We may divulge individual data to any individual performing review, lawful, operational, or different services for us. We will utilize data which does not identify the person for these exercises at whatever point achievable. Information divulged to vendors or contractors for operational purposes may not be re-disclosed to others by such a vendor or contractor. We may reveal individual data when needed to do as such by a court request or court order. We may divulge individual data as we esteem it proper to secure the safety of our customers or for an investigation identified with public safety or to report an activity that has all the earmarks of being disregarding the law. We may divulge individual data to ensure the security and dependability of this site and to take safety measures against accountability.

8.2 Disclosures to Third Parties

Personal information accessible through fcmb.com, including data held or processed by us or by you, may be subject to the legal and regulatory frameworks of the jurisdictions in which such data is stored, accessed, or transferred. As a result, this data may be disclosed in accordance with the laws applicable in those jurisdictions.

In compliance with legal and regulatory obligations, we may disclose your personal and financial information to regulatory authorities, law enforcement agencies, internal and external auditors, or legal representatives—whether in connection with supervisory reviews, investigations, audits, or as otherwise required by law.

8.3. International Data Transfer

In certain instances, your personal data may be transferred to third-party service providers or partners located outside Nigeria. Such transfers will only occur where necessary and in compliance with applicable data protection laws. We ensure that any international transfer of personal data is conducted with adequate safeguards by relying on legally mandated

instruments for authorized data transmission across borders, as recognized by the Nigeria Data Protection Commission (NDPC)

9. Information Security and Retention

At FCMB, we are committed to safeguarding the personal information we collect. We maintain robust administrative, technical, and physical safeguards designed to prevent loss, theft, unauthorized access, disclosure, copying, misuse, or alteration of personal data.

Our security measures include secure servers, firewalls, encryption protocols, and restricted access, granted only to employees who require the information to perform their official duties.

If you use a password for any of your accounts, you are responsible for keeping it confidential and should avoid sharing it with anyone.

We adhere to these principles to uphold the confidentiality, integrity, and availability of your personal information. While no method of transmitting data over the internet is entirely secure, we take all reasonable steps to protect your data.

We retain personal information only for as long as necessary to provide our services or to meet legal, regulatory, and operational requirements. Where an account is closed, certain information may still be retained to comply with legal obligations and to detect, monitor, and prevent fraud, only for as long as permitted by applicable laws, regulations, or FCMB's internal policies

9.1 Data Protection on the Internet

At FCMB, we utilize encryption technology to protect the transmission of data to or from you via fcmb.com. For security purposes, access to fcmb.com is restricted to authorized users only. However, because your information, account data, and other transactions may be accessed through a public network—the Internet—we cannot guarantee absolute security. You acknowledge and accept the risk that unauthorized persons may potentially access such information. If you suspect that your information has been compromised or accessed by an unauthorized party, please contact the Bank immediately

10. Customer Consent

Please refer to the end of this notice to provide your consent. You may withdraw your consent to the collection and processing of your personal data at any time by notifying us via our contact page. For individuals under the age of 18, consent must be provided by a parent or legal guardian. Kindly note that if you choose not to provide consent or withdraw it at any point, we may be unable to provide the requested services

11. Changes to our Privacy Policy

We may update this Privacy Policy periodically to reflect changes in our services or applicable data protection requirements. All updates will be posted on this page. Where any changes materially affect you, we will provide additional notice, such as through our website or by email. Continued use of our services following such changes will constitute your acceptance of the revised Privacy Policy

12. How to Contact us

For issues relating to personal data, please contact us via any of the below.

Corporate Address: Primrose Tower, 17A, Tinubu Street, Marina, Lagos

Telephone: 07003290000, 02012798800.

Email: dataprotection@fcmb.com AND customerservice@fcmb.com

WhatsApp: (+234) 09099999814 or (+234) 09099999815

Responsibility

As a customer, you accept this Privacy Policy when you sign up for, access, or use our products, services, content, features, technologies, or functions offered on our website, as well as all related sites, applications, and services (collectively referred to as “FCMB Services”).

This Privacy Policy governs the use of FCMB Services by all users, including those who engage with these services during their trade, practice, or business, unless otherwise agreed under a separate contract. Users have the right to exercise their data protection rights as outlined under the 'Customer Data Protection Rights' section of this Privacy Policy.

13. Data Protection Governance

FCMB has appointed a qualified Data Protection Officer (DPO) and maintains a Data Protection Compliance Organization (DPCO) relationship, in accordance with the NDPA.

We conduct mandatory annual audits and submit regulatory filings to the NDPC as required.

We integrate data ethics, inclusive design, and digital rights awareness in our digital innovation and transformation strategy.