TERMS AND CONDITIONS

Effective Date: November 2025

Last Updated: August 2026

Welcome to Embedly (the "Platform"), a product and application provided by Sterling Bank Ltd ("We," "Us," or "Our") designed to facilitate embedded financial experiences for businesses, ecosystems, and their respective customers (the "Services"). These Terms and Conditions ("Terms") govern your access to and use of the Platform.

By accessing or using the Platform, you acknowledge that you have read, understood, and agree to be bound by these Terms. These Terms constitute a legally binding agreement between you and Sterling Bank Ltd. If you do not agree to these Terms, you are prohibited from accessing or using the Platform and its Services.

DEFINITIONS

In these Terms, the following terms shall have the meanings ascribed to them:

- **Embedly/Platform** refers to the suite of infrastructure products and APIs offered by Sterling Bank Ltd under Embedly.
- **Device Binding** means the process of securely associating a user's wallet or application profile with a single trusted mobile device for security purposes.
- **Instant Payment (NIP)** means real-time electronic funds transfers processed through the Nigeria Inter-Bank Settlement System (NIBSS) Instant Payment Scheme or any successor payment infrastructure approved by the Central Bank of Nigeria.
- **Multi-Factor Authentication (MFA)** means the use of two (2) or more independent authentication factors to verify a user's identity before granting access to an account or authorising a transaction. Authentication factors may include, but are not limited to:
    - Password;
    - Transaction PIN;
    - One-Time Password (OTP);
    - Biometric Authentication;
    - Soft Token;
    - Hard Token; and
    - Liveness Verification.
- **User/Client/You** refers to any individual, business, or entity that accesses or uses the services provided through Embedly.
- **Services** include, but are not limited to, wallet creation, card issuance, payout APIs, and any other financial infrastructure services offered through the Platform.
- **Transaction Limit** means the maximum value of Instant Payment transactions permitted on a wallet or account over a specified period.
- **"Wallet Solution"**: A product made available by Embedly to facilitate the collection, storage, and disbursement of funds by Merchants, which may be Open, Closed or a checkout wallet.
- **"Applicable Laws":** All laws, regulations, guidelines, and circulars in force in Nigeria, including but not limited to CBN directives, NDPA 2023, Cybercrimes Act 2015 (As amended), and AML/CFT regulations.

USE OF THE PLATFORM

You agree to use Embedly only for lawful purposes and in accordance with these Terms. You are solely responsible for all actions and activities that occur under your account, and you must not misuse the Platform or attempt to access areas of the system that you are not authorized to access.

ELIGIBILITY

To access and use the Platform, you must be at least 18 years old and have the legal capacity to enter a binding contract. If you are using the Platform on behalf of an organization, that organization must be duly registered and authorized to operate within the jurisdiction in which it is based.

USER OBLIGATIONS

As a user of the Platform, you agree to the following:

- It is your sole responsibility to keep your Embedly account safe: Security Details, PIN and any part of your account security should not be shared with anybody else or carelessly stored or disclosed under any circumstance.
- If you leave your electronic access device without logging out, write your PIN down in a public space or share your details with anybody, we will not be liable for any errors, or results that may come of it.
- We will always use all reasonable efforts to keep the App and service safe, and your security settings will help us narrow it further down. However, if these issues arise due to carelessness with any part of your account security, there is very little we can do, and we will be relieved of any liability as regards the occurrence of a breach
- If you believe or reasonably suspect that there is a fraudulent act we haven't caught, it is your duty to notify us immediately. We will then investigate and report back to you through the most secure channel you provide to us.
- You are required to change your security options if you believe any part of your security has been compromised.
- Where you notify us of your intention to change your password, PIN or security options, we will, with your approval, delete these details and allow you set up new ones.
- After initial sign up, we will not contact you (or ask anyone to do so on our behalf) with a request to disclose your log in details or transaction password/PIN. If you receive any such request from anyone (even if they are using our name and logo and appear to be genuine) then it is likely to be fraudulent and you must not provide your log in details to them under any circumstances. Also, you should report any such request to us immediately.
- Comply with all applicable laws and regulations, including data protection laws, anti-money laundering regulations, and any other laws governing financial services in your jurisdiction.
- Not engage in any unlawful or fraudulent activity through the Platform or misuse the services in any way.

Security Controls

Users agree to:

- use only registered devices when accessing wallet services;
- immediately notify Embedly where a registered device has been lost, stolen or compromised;
- complete Multi-Factor Authentication whenever requested before any security-sensitive activity, including but not limited to:
    - increasing transaction limits;
    - enabling Instant Payment services;
    - device migration;
    - account reactivation;
    - security credential reset.

PRODUCTS & SERVICES

Embedly offers a variety of financial infrastructure services, including but not limited to:

- **Wallet Creation**: We enable the creation of wallets through Sterling Bank

  Where you apply to open or reactivate an Open Wallet online, we may, in accordance with applicable law and regulatory requirements:

  - validate your identity information in real time against the Bank Verification Number (BVN) and/or National Identification Number (NIN) databases;
  - subject the online opening of your Open Wallet to mandatory liveness verification;
  - implement enhanced authentication measures, including Multi-Factor Authentication (MFA), biometric authentication, One-Time Password (OTP), soft token, hard token, facial verification, or any other authentication mechanism required by applicable law or regulatory requirements; and
  - delay activation or reactivation of your Open Wallet until all required verification and authentication checks have been successfully completed.

  Default Transaction Limits

- Newly created open wallet shall have a maximum transaction limit of ₦20,000 during the first twenty-four (24) hours following account creation or wallet activation, as applicable.
- Existing open wallets activated on a newly registered device shall also be subject to a maximum transfer limit of ₦20,000 during the first twenty-four (24) hours following activation.
- Embedly reserves the right to impose lower limits based on fraud risk.
- **Payout Services**: Facilitate transfers in and out of wallets, enabling businesses to make payments to customers or suppliers.
- **Card Issuance**: Embedly provides access to physical or virtual cards through a Cards-as-a-Service model.
- **API Access**: Developers and businesses can integrate with Our API endpoints to build seamless financial products.
- **Merchant Compliance Obligations**
  Merchants integrating with Embedly agree, in relation to Open Wallets where applicable, to:

  implement all security APIs provided by Embedly;
  implement Embedly's Liveness Verification API for all online Open Wallet opening processes;
  integrate Device Binding functionality;
  integrate Instant Payment Opt-In and Opt-Out APIs;
  implement transaction limit management APIs;
  ensure that Customers requesting transaction limits above N500,000 complete Multi-Factor Authentication and, where applicable, Enhanced Due Diligence (EDD) and identity verification checks, and provide such customer information and supporting documentation as may be required to complete these checks; and
  notify customers of applicable regulatory security restrictions.

  In addition, Merchants shall:

  maintain adequate fraud prevention controls;
  cooperate with regulatory investigations; and

comply with all applicable laws, regulations, and future CBN payment system directives.
Failure to comply may result in immediate suspension of API access.

- **Account Management Tools**: Users gain access to various tools for managing their accounts, including dashboards, sandbox environments, and detailed developer documentation.
- **Instant Payment Security Controls**
  Where a Merchant enables Instant Payment services through Embedly, the following minimum controls shall apply:

    - Instant Payment shall be enabled by default for newly onboarded customers.
    - Customers may voluntarily opt out of Instant Payment at any time.
    - Customers may subsequently opt back into Instant Payment at any time.
    - All opt-in and opt-out requests must be authenticated using Multi-Factor Authentication.
    - During an opt-out period customers shall not be permitted to perform online Instant Payment transfers.
    - Transfers may only resume after successful opt-in.

Enterprise Fraud Monitoring

Embedly may implement automated enterprise fraud monitoring systems to monitor wallet activity, inbound and outbound transactions for fraud detection, regulatory compliance and risk management purposes.
Users acknowledge that Embedly may:

- temporarily suspend transactions;
- reduce transaction limits;
- require additional authentication;
- delay settlement;
- request additional KYC documentation, Know Your Business (KYB), or other due diligence documentation; and
- take any other reasonable measures necessary to protect users, the Platform, Sterling Bank Ltd, or to comply with applicable laws and regulatory requirements.

Customer Disclosure
Merchants shall ensure that Customers are notified, in relation to Open Wallets, that:

Instant Payment functionality is enabled by default for newly onboarded Customers;
Customers may voluntarily opt out of Instant Payment services at any time;
Customers may subsequently opt back into Instant Payment services after successful Multi-Factor Authentication;
Customers who opt out will be unable to initiate online Instant Payment transactions until they successfully opt back in; and
Certain security restrictions, including temporary transaction limits, are mandatory regulatory controls and cannot be waived

Customer Transaction Limit Management

Customers may voluntarily request to:

- increase transaction limits;
- reduce transaction limits;

subject to:

- successful Multi-Factor Authentication;
- fraud screening;
- applicable regulatory limits;
- Embedly's risk assessment;
- implementation of Sterling Bank's risk assessment framework and any other applicable requirements or documentation provided to Merchants; and any requirements imposed by Sterling Bank or the Central Bank of Nigeria.

Embedly and/or Sterling Bank may approve, reject or defer any requested increase or reduction following enhanced due diligence, fraud screening and applicable regulatory requirements.

Device Registration and Binding

Merchants shall ensure that Customers complete device registration and binding requirements in accordance with Embedly's security requirements before accessing applicable services.

For security purposes:

- Wallet applications may only be registered and active on one mobile device at any given time.
- Registering or migrating to a new device may deactivate previously registered devices and shall require re-authentication in accordance with applicable regulatory requirements.
- Embedly may temporarily reduce transaction limits following device migration.
- Customers shall be informed of and acknowledge that security restrictions imposed following device migration are regulatory requirements and not service failures.

MODIFICATIONS TO THE TERMS

- We may change these terms from time to time. Where the revision is **material** (including changes to price, fees, payment terms, limits of liability, or your core rights), we will give you prior reasonable notice on the Platform setting out the changes and the effective date. Changes will be effective when posted on the Platform with the revised Terms indicating the effective date of the changes with no other notice provided. Your continued use of the Platform after any modifications have been posted constitutes your acceptance of the updated Terms. Please check the Terms regularly for updates as changes shall be effective immediately, and we may indicate the date of such revision.

- In addition, we may change, suspend or discontinue any aspect of the Services at any time. We may also impose limits on certain services or restrict your access to parts or all of the Platform or the Services provided with notice to you, to the extent practicable within the law and existing banking regulations.

- You are free to decide whether or not to accept a revised version of these Terms, but accepting these Terms, as revised, is required for you to continue accessing or using the Platform and Services. If you do not agree to these Terms or any revised version of these Terms, your sole recourse is to terminate your access or use of the Services. Except as otherwise expressly stated by us, your access and use of the Services are subject to, and constitute your acceptance of, the version of these Terms in effect at the time of your access or use.

ADDITIONAL TERMS

- **Electronic Communications**: By using the Platform, you consent to receive all communications, notices, disclosures, and agreements electronically. These electronic communications satisfy any legal requirements for written communication.
- **Feedback Release**: We may from time to time reach out to Clients/Users to provide feedback/testimonials in respect of our Services and/or the Platform. This would usually involve the use of your images, biographical information, recordings, video/audio clips (the "Material"). You acknowledge that the Material may be used in diverse settings within an unrestricted geographic area. You hereby release Sterling Bank Limited, its representatives, employees, managers, members, officers, parent companies, subsidiaries, and directors, from all claims and demands arising out of or in connection with any use of the Material, including, without limitation, all claims for invasion of privacy, infringement of your right of publicity, defamation and any other personal and/or property rights. Additionally, you waive any right to royalties or other compensation arising or related to the use of the Material.

UNAUTHORIZED DEBITS IN OPEN WALLET SYSTEMS

Prohibition of Unauthorized Debits from Customer Wallets (Open Wallet Merchants Only)

To protect consumers and uphold regulatory compliance under the Central Bank of Nigeria (CBN) Consumer Protection Framework and the Regulatory Guidelines for Open Banking, all merchants operating open wallet systems via the Embedly platform are expressly prohibited from initiating wallet-to-wallet transfers or debiting a customer's wallet without first obtaining the customer's explicit, informed, and verifiable consent.

Such consent must be collected through secure and traceable methods, including but not limited to:

- One-Time Password (OTP) authorization,
- Biometric validation, or
- Secure in-app confirmations.

This prohibition applies exclusively to open wallet systems, defined as wallets capable of interfacing with multiple third-party platforms. It does not apply to closed wallet systems that operate within a self-contained, single ecosystem.

Any unauthorized debit by an open wallet merchant shall constitute:

- A material breach of these Terms,
- A regulatory violation under applicable CBN rules, and
- A trigger for enforcement action as described below.

In the event of such a breach, the offending merchant shall:

1. Fully indemnify Us against all resulting liabilities, including but not limited to regulatory sanctions, third-party claims, legal fees, and reputational damage.
2. Be subject to immediate suspension, potential blacklisting, and regulatory escalation to the Central Bank of Nigeria (CBN), Nigeria Inter-Bank Settlement System (NIBSS), or other relevant bodies.
3. Ensure full restitution to the affected customer(s) within 72 hours of detection or notice; and
4. Pay a non-negotiable penalty of ₦5,000,000 (Five Million Naira) per incident.

We reserve the right to carry out routine or ad-hoc compliance reviews and audits to ensure strict adherence to this policy. Non-compliance will be treated with the highest level of severity under these Terms.

Closed Wallet Solution (Applicable only to Merchants authorised by Sterling Bank Ltd to operate Closed Wallets)

1. **Nature of the Closed Wallet**

- The Closed Wallet is a merchant-owned and merchant-controlled wallet created under the Embedly platform.
- The wallet shall be used solely to collect funds from customers for products and services rendered by the Merchant.
- The wallet is not a bank account or a customer-managed e-wallet.

3. Customer Disclosure and Consent

- The Merchant agrees that all customers using the closed wallet must be fully aware that the wallet is a collection tool for the Merchant and not a wallet under their personal ownership or control.
- The Merchant shall ensure that customers provide informed consent to any transaction that results in a debit to their account.

4. Obligation to Provide Value Before Debit

- The Merchant shall ensure that value (product, service, or benefit) is delivered or guaranteed to the customer prior to initiating a debit on the customer's account via the closed wallet system.

5. Liability and Risk Allocation

- The Merchant acknowledges and agrees that it is solely responsible for all activity on its closed wallet, including fraud, misappropriation, misuse, unauthorised debits, or disputes arising from customer transactions.
- Embedly bears no responsibility for the Merchant's actions, omissions, or handling of customer funds.
- The Merchant agrees to indemnify, defend, and hold harmless Sterling Bank Ltd, its directors, employees, agents, and affiliates from and against any and all claims, losses, damages, liabilities, penalties, costs, and expenses (including legal fees) arising out of or relating to any failure to provide value to customers, customer disputes, fraudulent or unauthorised transactions or breach of this Agreement.

6. Monitoring, Compliance and Audit

- We reserve the right to periodically audit the Merchant's compliance with Closed Wallet operations.
- The Merchant shall maintain adequate technical and organisational controls to prevent fraud and unauthorised transactions.

7. Fraud, Misappropriation and Breach

- Upon any indication of fraud, misuse or breach of the Closed Wallet framework, we may immediately suspend or terminate the Wallet.
- We may hold back or withhold any funds collected until full investigation is concluded.
- Merchants shall fully cooperate with all investigations and promptly refund affected customer value if required.

8. Regulatory Compliance

- The Merchant agrees to comply with all applicable laws, including the CBN Consumer Protection Framework, the Nigeria Data Protection Act 2023, AML/CFT obligations, and any other applicable regulations.
- Failure to comply shall entitle Us to suspend or terminate the Merchant's access to the Closed Wallet Solution.

9. Termination

- We may terminate access to the Closed Wallet without notice in cases of fraud, breach of these Terms, or regulatory directives.
- In non-material breach scenarios, we shall give seven (7) days' notice to remedy such breach before termination.

MONEY LAUNDERING & COMPLIANCE

You represent and warrant that you will not engage in any activity that involves money laundering, fraud, or illegal sources of funds. You agree to comply with all applicable Know Your Customer (KYC), Know Your Business (KYB) and Anti-Money Laundering (AML) requirements. Upon request, you will provide all necessary documentation to verify your identity and business activities. Additionally, you agree to allow Sterling Bank Ltd monitor transactions, report suspicious activities to relevant authorities, and comply with all applicable regulations, including those enforced by the Central Bank of Nigeria.

SUSPENSION OF THE PLATFORM/SERVICES OR YOUR ACCOUNT

We reserve the right to suspend your access to the platform/service, or any feature thereof on one or more of the following grounds:

- To protect the security, integrity, or stability of the platform or our systems.
- If we suspect fraud, unauthorized access, or suspicious activity on your account.
- If you fail to comply with security protocols (eg, authentication requirements).
- Violation of these Terms and Conditions or any agreement you have with us.
- Where you provide false, misleading, or incomplete information to us.
- Where there is a reasonable suspicion of your involvement in, or attempted illegal activity (e.g., money laundering).
- Where we find or reasonably suspect that you have provided false information to us, or misrepresented your identity
- Your failure to meet AML/CFT, KYC or other regulatory requirements.
- In compliance with legal/regulatory orders (e.g., CBN directives, court rulings).
- To carry on scheduled or emergency maintenance, upgrades, or technical disruptions.
- Where you no longer meet eligibility criteria for use of the platform/service (e.g., closed account, unsupported device).

- Upon our receipt of a notice of bankruptcy, or legal incapacity.
- Where the platform is no longer made available by the App store in your location
- Your device/IP is flagged by cybersecurity partners (e.g., for malware).
- Prolonged negative balance or failure to settle fees linked to digital services.
- Excessive or fraudulent transaction disputes on your account
- Unusual patterns on your account that trigger internal risk thresholds
- Where we determine that the relationship with you or your continued use of the platform/service represents increased risk of loss or liability to us
    - We may impose temporary security restrictions on Instant Payment functionality where:
    - you elect to opt out of Instant Payment services;
    - a device migration requires re-authentication under applicable regulatory requirements;
    - enhanced fraud monitoring identifies unusual or suspicious activity; or temporary transaction limits are imposed in accordance with applicable law or regulatory requirements.

We will provide adequate prior notice of suspension of the service. However, we may suspend access to the service immediately, where such immediate action is required to mitigate risks (e.g., fraud, security threats), or where an advance notice is prohibited by law or may signal "tipping-off" or where advance notice may harm the platform, other users of the platform, or ongoing investigations.

CLOSING YOUR ACCOUNT

You have the right to deactivate or permanently close your account at any time. If you wish to close your account, please contact us using the information provided in the "Contact Us" section. Upon account closure, you will no longer have access to the services provided through the Platform, and all outstanding balances and obligations will remain due.

DISCLAIMERS

- While we strive to provide reliable and secure Platform, you acknowledge that the Platform may occasionally be unavailable due to necessary maintenance, upgrades, or circumstances beyond our reasonable control. We will provide advance notice of scheduled interruptions where practicable, but cannot guarantee uninterrupted service availability. The Platform and all related services are provided on an "as available" basis, and we disclaim liability for any losses arising from service unavailability, except where such unavailability results from our gross negligence or willful misconduct.
- The Platform may integrate or provide access to third-party services for your convenience. While we exercise due care in selecting third-party providers, we do not guarantee or assume responsibility for their services, content, or actions. Your use of any third-party services is at your own risk, and we recommend reviewing the terms and privacy policies governing such services. However, we remain responsible for our own negligence in selecting or overseeing these third-party providers.

- To the fullest extent permitted by applicable law, we disclaim all implied warranties including merchantability or fitness for particular purpose, while affirming our commitment to providing services with the professional skill and care expected of a licensed financial institution under CBN regulations. Nothing in these terms shall limit or exclude our liability for death or personal injury caused by our negligence, fraud, or any other liability that cannot be lawfully limited or excluded under Nigerian law.
- Our liability for direct losses arising from breach of these terms or negligence shall be limited to the fees you paid for the affected services in the preceding twelve months. We shall not be liable for any indirect, consequential, or special damages, including but not limited to lost profits, data loss, or business interruption, except where such limitation is prohibited by law. This disclaimer does not affect your statutory rights under the CBN Consumer Protection Regulations or other applicable Nigerian laws.

RESOLUTION RESPONSE TIME AND ESCALATION PROCEDURE

Issue Severity	Description	Response Time	Resolution Time	Escalation Procedure
Critical	Platform down or services unavailable.	Within 1 hour	Within 2 business days	Customer Support → Technical Support → Engineering Team → Management Team
High	Major issues affecting platform usability, but not entirely down.	Within 1 hour	Within 1 business day	Customer Support → Technical Support → Engineering Team
Medium	Non-urgent issues with functionality or minor disruptions.	Within 1 hour	6-12 Hours	Customer Support → Technical Support
Low	General inquiries or minor issues.	Within 1 hour	3-6 Hours	Customer Support

ESCALATION PROCESS

Level	Description	Responsible Team	Action/Procedure
Customer Support	First point of contact for all issues and general inquiries.	Customer Support Team	Provide initial troubleshooting, answer questions, gather details for escalation if needed.
Technical Support	Handles technical or system-related issues that cannot be resolved by customer support.	Technical Support Team	Investigate platform functionality, resolve bugs, and issues related to features.
Engineering Team	For critical, complex, or unresolved issues requiring development resources.	Engineering Team	Handle deep technical issues, platform bugs, and security vulnerabilities.
Management Team	For urgent, unresolved issues or if a dispute needs higher-level intervention.	Management/Operations Team	Assess critical issues and make strategic decisions to resolve escalated cases.

INTELLECTUAL PROPERTY

You agree that all intellectual property rights and database rights, whether registered or unregistered, in the Platform, information content on the Platform and all the website designs, including, but not limited to, text, graphics, software, photos, video, music, sound, and their selection and arrangement, and all software compilations, underlying source code and software shall remain at all times vested in us or our licensors. Use of such material will only be permitted as expressly authorized by us or our licensors. Any unauthorized use of the material and content of this Platform is strictly prohibited, and you agree not to, or facilitate any third party to, copy, reproduce, transmit, publish, display, distribute, commercially exploit, or create derivative works of such material and content.

CONFIDENTIALITY

In the course of providing you with services on the Platform, we are committed to adhering to all relevant Data Protection Laws, including but not limited to Nigeria Data Protection Act 2023 (NDPA), European Union General Data Protection Regulations (GDPR) and any other applicable regulations governing the handling and protection of personal data. We take the confidentiality and security of your information seriously and implement robust security measures to safeguard your personal and sensitive data.

We make reasonable efforts to ensure the confidentiality and integrity of the information you share with us. This includes the use of encryption, access controls, and regular security assessments to prevent unauthorized access, disclosure, alteration, or destruction of your data.

THIRD-PARTY SERVICE PROVIDERS

To ensure the proper functioning of the Platform, we may engage trusted third parties to perform specific functions essential to your use of the services. These third parties may include cloud service providers, payment processors, hosting companies, and other technical or operational service providers. By using our Platform, you consent to the sharing of your confidential information with these third parties as necessary for the provision of services.

We take steps to ensure that any third-party service providers we engage are bound by appropriate contractual agreements to maintain the confidentiality and security of your data. These agreements ensure that third parties are only permitted to use your data in ways that are necessary to perform their specific tasks and functions in accordance with our obligations under applicable law.

DATA SECURITY MEASURES

We implement industry-standard security measures to protect your data against unauthorized access, alteration, or loss. This includes encryption of sensitive data both in transit and at rest, the use of secure authentication mechanisms, and the application of regular software patches and updates to address potential vulnerabilities.

While we strive to ensure the highest levels of data protection, it is important to note that no system is completely secure. As such, we cannot guarantee absolute protection against data breaches or unauthorized access, but we are committed to continuously improving our security practices to mitigate such risks.

RETENTION OF DATA

We retain your personal data only for as long as necessary to fulfil the purposes for which it was collected, including for legal, accounting, or reporting requirements. Once the data is no longer needed for the purposes it was collected for, it will be securely deleted or anonymized.

USER RESPONSIBILITY

While we take measures to protect your data, it is also important that you take responsibility for maintaining the confidentiality of your account credentials, including passwords and security questions. You should promptly notify us of any unauthorized access or use of your account.

COMPLIANCE WITH LEGAL REQUESTS

In the event of a legal request or a governmental investigation, we may be required to disclose your personal information to comply with applicable laws or regulations. We will make reasonable efforts to notify you in such cases unless prohibited by law or court order.

ASSIGNMENT

You may not assign or transfer your rights or obligations under these Terms to any third party without our prior written consent. We reserve the right to assign or transfer our rights and obligations under these Terms without notice to you.

INDEMNITY

You agree to indemnify and hold harmless Embedly (Sterling Bank Ltd), its affiliates, officers, directors and employees from any claims, damages, losses, liabilities, or expenses (including legal fees) arising from:

- Your use of the Platform,
- Your violation of these Terms,
- Your breach of applicable laws,
- Any fraudulent, negligent, or willful misconduct.
- Any unauthorized use or access resulting from the Partner's failure to safeguard its API Key.
- Any breach of applicable law or regulation arising from the unauthorized use of the API.
- Any third-party claim resulting from data exposure, fraud, or other malicious activity tied to the use of Partner's credentials.

LIMITATION OF LIABILITY

To the fullest extent permitted by law, neither Sterling Bank Ltd nor its affiliates shall be liable for any indirect, incidental, special or consequential damages arising from:

- your use or inability to use the Platform;
- regulatory security restrictions imposed in compliance with applicable law;
- mandatory fraud prevention controls;
- temporary transaction limits;
- mandatory authentication requirements;
- device binding controls; or
- your voluntary election to opt out of Instant Payment services,

except where such loss results from our negligence, fraud, willful misconduct or any liability that cannot lawfully be excluded under applicable Nigerian law

.FORCE MAJEURE

To the fullest extent permitted under applicable law, we will be excused from performance under these Terms for any period that we are prevented from or delayed in performing any obligations pursuant to this Terms, in whole or in part, as a result of a Force Majeure Event. For purposes of this section, "Force Majeure Event" means an event or series of events caused by or resulting from any of the following: (a) weather conditions or other elements of nature or acts of God; (b) acts of war, acts of terrorism, insurrection, riots, civil disorders or rebellion; (c) quarantines or embargoes, (d) labor strikes; (e)~~;~~ unauthorized access to our information technology systems by third parties; or (f) other causes beyond our reasonable control and contemplation.

WAIVER

Any failure by Sterling Bank Ltd to enforce any provision or condition set forth in these Terms shall be deemed a further or continuing waiver of such term or condition or a waiver of any other term or condition, and any failure by us to assert a right or provision under these Terms shall not constitute a waiver of such right or provision.

SEVERABILITY

If any provision of these Terms is found to be invalid, illegal, or unenforceable, the remaining provisions shall remain in full force and effect. The invalid provision will be replaced with a valid provision that most closely matches the intent of the original provision.

GOVERNING LAW AND DISPUTE RESOLUTION

These Terms shall be governed by and construed in accordance with the laws of the Federal Republic of Nigeria. Any dispute arising out of or in connection with these Terms that cannot be resolved amicably within thirty (30) days shall be submitted to mediation at the Lagos Multi-Door Courthouse (LMDC), in accordance with the Lagos State Multi-Door Courthouse Law 2007 (or its extant law).

CONTACT US

If you have any questions or concerns about these Terms, please feel free to reach out to us:

- **Email**: Embedlycs@embedly.ng
- **Phone**: +234 707 550 1198

ACCEPTANCE OF THESE TERMS

By accessing or using the Platform, you acknowledge that you have read, understood, and agree to be bound by these Terms and Conditions. If you do not agree to abide by these Terms, you are not authorized to access or use the Platform.