FCMB Regal Rewards Incident Management Policy and Procedure

1. Introduction

The FCMB Regal Rewards platform, operated in partnership between First City Monument Bank (FCMB) and Regal Cards Nigeria Ltd ("Regal Cards", "we", "our", or "us"), is a secure digital platform designed to offer premium lifestyle perks to FCMB customers. As a platform built on the Wix ecosystem and integrated with FCMB's internal infrastructure, we recognize that information security incidents—whether accidental or malicious—can pose a risk to data integrity, customer trust, and regulatory compliance.

This Incident Management Policy and Procedure document outlines the principles, protocols, and responsibilities involved in identifying, managing, mitigating, and reporting any security or privacy incidents that may occur in the FCMB Regal Rewards platform. It also outlines how we fulfill our legal obligations under the Nigeria Data Protection Act (NDPA) and the guidelines of the Nigeria Data Protection Commission (NDPC).

We acknowledge the importance of ensuring that all incidents, no matter how minor they may appear initially, are handled swiftly, transparently, and effectively, with clear communication to all stakeholders involved, especially FCMB as the data controller.

2. Purpose of This Document

The primary purpose of this document is to:

- Establish a structured approach to incident detection, response, and recovery.
- Ensure timely communication and escalation of incidents to FCMB and other relevant authorities when required.
- Minimize the operational, reputational, and legal impacts of data-related incidents.
- Maintain a clear audit trail of all incident management activities.
- Ensure compliance with the NDPA 2023, the General Data Protection Regulation (GDPR) where applicable, and internal FCMB risk policies.

3. Scope of Application

This Incident Management Policy applies to:

- All services offered on the FCMB Regal Rewards platform including concierge, bookings, merchant rewards, and chat functions.
- All personal data processing activities conducted by Regal Cards on behalf of FCMB.
- All staff and vendors with access to backend administrative functions or customer support.
- All system components and infrastructure, including Wix-hosted databases, chat integrations, and payment processors.
- Sub-processors, such as the FCMB payment gateway.

4. Definition of an Incident

For the purpose of this policy, an incident is defined as any event that:

- Compromises or potentially compromises confidentiality, integrity, or availability of customer data.
- Results in unauthorized access, alteration, deletion, or disclosure of personal information.
- Interrupts or degrades the platform's normal operation in a way that could affect customer service.
- Violates privacy laws, internal policies, or customer expectations.

Examples of incidents may include:

- Accidental exposure of user emails or contact details.
- Unauthorized access to backend systems by an unapproved party.
- Payment gateway outage or error during customer transactions.
- Live chat system compromise or misrouting of sensitive customer requests.

4.1 Definitions

- **Incident:** Any actual or suspected event that may impact data confidentiality, integrity, or availability.
- **Data Breach:** A confirmed incident where personal data is exposed to unauthorized individuals or systems.
- **P1 Incident:** Critical issue affecting customer data integrity, platform availability, or resulting in a breach.
- **P2 Incident:** Medium-level issue that affects user experience but has no data breach implications.
- **P3 Incident:** Low-priority technical anomalies or bugs.

5. Roles and Responsibilities

Regal Cards Nigeria

- Maintain a designated Data Protection Officer (DPO) responsible for overseeing incident response.
- Operate an Incident Response Team (IRT) to handle reports, triage, and resolution.
- Log and track all incidents with timestamps, affected systems, and actions taken.
- Notify FCMB within the specified window of detection for all notifiable incidents.

FCMB

- Oversee the execution of data control responsibilities.
- Receive notifications and incident summaries from Regal Cards.
- Determine if external reporting to NDPC or affected customers is warranted.

5.1. Roles and Responsibilities

Role	Responsibility
Incident Response Team (IRT)	Regal Cards designated personnel responsible for executing the procedures.
Data Protection Officer (DPO)	Ensures incidents involving personal data are assessed, reported to NDPC, and remediated.
FCMB Technology Team	Informed of all major incidents, supports remediation and oversight.
Wix Platform Support	Provides technical incident resolution for infrastructure-related issues.
Third-party Vendors (e.g., Payment Gateway)	Must notify the IRT of any incident that affects FCMB Regal operations or customer data.

6. Incident Detection

Incidents may be detected by:

- Internal monitoring systems (e.g., login alerts, failed authentication attempts).
- Live chat logs or customer reports indicating suspicious activity.
- Automated logs from Wix or email service integrations.
- Manual reports from FCMB teams, customers, or partners.

All reports are recorded immediately into a centralized incident log hosted on secure internal systems. Initial classification is carried out within 30 minutes of report where possible.

7. Incident Classification

Incidents are categorized as follows:

- Low: No customer impact, internal system notice only.
- Medium: Temporary customer disruption or contained exposure (e.g., live chat misrouting).
- High: Widespread data exposure or unauthorized access with privacy implications.
- Critical: Platform-wide compromise, ransomware, or breach of multiple systems or customer records.

The classification dictates the speed of escalation and nature of FCMB involvement.

7.1. Types of Incidents Covered

- Unauthorized access attempts
- Data breaches or leaks
- Website defacement or denial of service
- System outages or degraded performance
- Login/session hijacking
- Malicious software (malware/phishing)
- Loss or theft of customer data
- Internal staff misconduct impacting data privacy

8. Incident Response Timeline

1. Initial Detection: Incident is logged and assessed.
2. Classification: The incident is categorized within 30–60 minutes.
3. Immediate Containment: Temporary lockdown or data isolation steps taken.
4. Notification to FCMB: Within 4 hours for high/critical incidents, or 24 hours for low/medium.
5. Root Cause Analysis (RCA): Conducted and shared within 48–72 hours of containment.
6. Corrective Action: Implemented within 5 business days, if not sooner.

9. Communication Protocol

- Regal Cards will inform FCMB via secure email and/or phone once an incident is classified as reportable.
- If the incident involves customer data or brand equity, FCMB will determine whether further notification to NDPC or customers is required.
- All communications are logged and attached to the incident report record.

9.1. Incident Classification

Severity	Description	Response Time
P1	Data breach, unauthorized access to customer information	Immediate (<1 hour)
P2	Downtime without data compromise	Within 4 hours
P3	Cosmetic or low-impact issues	Within 24–48 hours

10. Root Cause Analysis (RCA)

After containment, a structured RCA process is conducted to determine:

- Why the incident occurred (e.g., expired credentials, third-party API error).
- Whether it was preventable, and if so, what control failed.
- What specific systems and customers were affected.
- Remediation timeline, ownership, and future safeguards.

The RCA is documented in a formal report, which is shared with FCMB within 72 hours of the incident being controlled.

11. Incident Response Procedure

Step 1: Initial Triage

- Acknowledge report and log incident in the internal tracker
- Assign an incident lead based on scope

Step 2: Containment

- For P1 incidents: restrict system access immediately
- Isolate affected components (e.g., freeze a chat plugin, redirect users to static maintenance page)

Step 3: Investigation

- Review logs on Wix backend and security plugin records
- Confirm impact scope
- Contact Wix support for infrastructure-related events

Step 4: Resolution

- Apply code patches, reconfigure access settings, restore backup data
- Verify integrity of personal data
- Notify affected customers (if breach involves personal data)

Step 5: Notification to NDPC (if applicable)

For data breaches affecting personal information:

- Notify NDPC within 72 hours with the following:
    - Nature of breach
    - Estimated volume and type of personal data exposed
    - Mitigation steps taken
    - Contact information of the DPO

Step 6: Communication

- Issue communication to FCMB team and management
- Draft customer communication with FCMB approval (for public-impacting incidents)

12. Post-Incident Review

After resolution, a Post-Incident Review (PIR) is conducted involving relevant Regal Cards personnel and FCMB stakeholders. This ensures:

- Lessons learned are captured.
- Policies or protocols are amended.
- Training needs are identified.
- Affected systems are monitored closely for a period.

13. Regulatory Notification

In cases where personal data is breached, Regal Cards will:

- Work with FCMB to determine the materiality threshold of the breach.
- Where necessary, assist FCMB in preparing a breach notification to NDPC within 72 hours as required by law.
- Ensure full transparency in root cause, impact, and resolution.

14. Record Keeping and Documentation

A full incident register is maintained securely and retained for a period of minimum 5 years. Each record includes:

- Incident summary and classification.
- Timestamps for each phase (detection to closure).
- Details of systems or customers affected.
- Communications, RCA, and final resolution status.

15. Training and Awareness

All staff managing or supporting the FCMB Regal Rewards platform undergo:

- Annual data protection training, covering incident response.
- Scenario-based simulations to improve response time and reduce errors.
- Refresher training whenever key policies are updated.

16. Review and Audit

This policy and procedure document is reviewed:

- Quarterly, in collaboration with FCMB.
- After any notifiable incident, to capture lessons learned.
- In the event of legal or regulatory changes to data protection laws.

Audit logs from Wix, chat systems, and backend admin tools are reviewed regularly to ensure policy adherence.

17. Contact and Escalation

If you detect or suspect an incident while using the FCMB Regal Rewards portal, please report it immediately to:

Data Protection Officer – Regal Cards Nigeria

Email: memebrship@regal.cards

Escalation may then proceed to FCMB's Data Protection and Risk Management team, based on severity and potential exposure.

Signed:

_____

Nnamdi Umezurike
Head of Partnerships
Regal Cards Nigeria

Effective Date: **01/07/2025**