19 Tambach Road, Sunninghill, Sandton,
Gauteng South Africa, 2191
support@enlbank.com
0860 111 372
www.enlbank.com

21 April, 2006

RE: Data Leakage Incident

Dear Mr. Geffen,

1. Acknowledgement and accountability

We would like to acknowledge that a security misconfiguration in a non-production environment led to the unintended exposure of certain data through a publicly accessible endpoint. As a bank, we remain fully accountable for the protection of customer information, regardless of whether systems are managed internally or by third-party service providers. We are formally treating this as a data leakage incident and are following all required reporting and notification processes. This includes engagement with:

- The Information Regulator (South Africa)
- The South African Reserve Bank
- Other relevant regulatory authorities

In line with our legal obligations, we will also notify affected customers directly.

2. Nature and scope of exposure

Our internal investigation has confirmed the following:

- The exposure originated from a User Acceptance Testing (UAT) environment used for reconciliation and reporting
- This environment was separate from our live production banking systems
- The issue was caused by a temporary firewall configuration lapse, which has since been corrected

Importantly:

- The data involved primarily relates to testing and reporting datasets except for the CODI-related reporting extracts which are based on current customer data
- The exposure was limited to a small number of customers (over 700)
- There is currently no evidence of widespread or systemic compromise of our production systems

3. Financial and card-related data

We understand your concerns regarding financial and card information and have looked into this

carefully. Our current assessment indicates that:

- Core production card systems and live transaction processing environments were not compromised
- The data referenced appears only in test and reconciliation datasets, not in active transactional systems
- A detailed forensic review is underway to validate all data fields, including any card-related information, to fully confirm risk exposure

Out of caution, we are approaching this matter with the highest level of diligence.

4. Immediate actions taken

As soon as we were notified, we took the following steps:

- Secured the affected server and removed it from public access
- Disabled all external access and file transfer mechanisms
- Migrated the environment to a secure, internally controlled platform
- Initiated a full investigation
- Implemented additional hardening and configuration controls across all environments

5. Governance, controls, and assurance

To provide context on our broader control environment:

- Our systems are continuously monitored as part of our operational and security processes
- We completed an independent audit in September last year, with satisfactory outcomes
- We maintain structured governance across information security, risk management, and data protection

While this incident highlights a specific control lapse in a non-production environment, it does not indicate a broader breakdown of our control framework. Nonetheless, we are using this as an opportunity to strengthen controls further, particularly for non-production and third-party-managed environments.

6. Third-party and environment context

The affected server supported:

- Finance and reconciliation processes
- CODI-related reporting requirements
- Payment system integration outputs

We would like to reiterate that third-party involvement does not reduce our accountability. As part of our response, we are reviewing:

- Third-party security controls
- Data handling practices
- Environment segregation and access management

7. Discovery and access

We acknowledge your observation that the data may have been accessible through publicly indexed services. Although no advanced intrusion techniques were required to discover it, we fully recognise the seriousness of this issue. Accordingly, we are:

- Confirming the duration of the exposure
- Assessing whether any unauthorised access occurred beyond what has been reported
- Enhancing our external exposure monitoring and threat-detection capabilities

8. Customer protection and next steps

Protecting our customers remains our highest priority. As part of our ongoing response:

- Affected customers will be contacted directly
- Enhanced monitoring and support measures are being implemented
- We are assessing whether additional safeguards, such as credential resets or extended monitoring services, are necessary

9. System upgrade context

As previously communicated to customers and regulators, we are currently undertaking a core system upgrade and broader technology transformation. This includes:

- Strengthening security architecture
- Improving separation between production and non-production environments
- Enhancing data governance and access controls

This incident has been incorporated into that programme to accelerate remediation and improvement efforts.

10. Closing

We take this matter seriously and remain committed to:

- Transparency with regulators and affected stakeholders
- Swift remediation and continuous control improvement
- Upholding the highest standards of accountability, ethical conduct, risk management, and operational resilience

We appreciate the opportunity to respond and will continue to cooperate fully as the investigation progresses.

Kind regards,
eNL Mutual Bank