PRELIMINARY INVESTIGATION BRIEF

Internal Audit Team, Finance Department

Date: August 10, 2022

Confidentiality Level: Internal Only

Risk Assessment Score: 50

Financial Impact USD: 787,806,540

Subject: Corporate Espionage and Data Breach Investigation: Initial Findings

As we delve into the complex web of corporate espionage and data breaches surrounding the investment fraud scheme at Veridian Bank, our preliminary investigation brief highlights the emerging scope of the issue, the initial evidence gathered, and the immediate concerns that demand attention.

Background:

In the midst of a heated power struggle, Veridian Bank's executives prioritized reputation over investigation, dismissing warnings from Evelyn Reed, the Head of Risk Management. Meanwhile, Marcus Thorne's Investment Division, responsible for managing the problematic Meridian Opportunities Fund, continued to operate with alarming autonomy. The stage was set for a catastrophic data breach.

Initial Findings:

Our investigation uncovered a sophisticated network of corporate espionage, involving the unauthorized transfer of sensitive information to a competitor, Titan Financial Group. Key findings include:

1. **Compromised Systems:** Our forensic analysis revealed that Thorne's Investment Division had installed a backdoor access point in the bank's network, allowing unauthorized access to high-risk transactions.
2. **Data Breach Incidents:** We identified multiple instances of data breaches, compromising client information and internal communications. The compromised data includes confidential client documents, employee records, and proprietary business information.
3. **Unusual Transaction Patterns:** Our review of transaction records revealed a series of unusual patterns, including sudden and unexplained transfers of large sums of money between internal accounts.

4. **Suspicious Communications:** We uncovered a series of cryptic emails and instant messages exchanged between Thorne and an external party, hinting at a coordinated effort to manipulate market dynamics.

Immediate Concerns:

The scope of the issue is far-reaching, with potential consequences extending beyond the bank's immediate interests. The following concerns demand urgent attention:

1. **Regulatory Scrutiny:** The Federal Banking Commission (FBC) and other regulatory bodies are likely to scrutinize Veridian Bank's governance and internal controls, potentially leading to severe penalties and reputational damage.
2. **Client Confidence:** The data breach and corporate espionage have compromised client trust, threatening the bank's ability to retain business and maintain market share.
3. **Employee Trust:** The compromised integrity of internal systems and processes has eroded employee trust, potentially leading to a mass exodus of key personnel.

Next Steps:

To address these concerns, we recommend the following immediate actions:

1. **Emergency Board Meeting:** Schedule an emergency board meeting to discuss the findings and outline a comprehensive response strategy.
2. **Enhanced Security Measures:** Implement enhanced security measures to safeguard internal systems and prevent future data breaches.
3. **Investigation Expansion:** Expand the investigation to include all parties involved in the corporate espionage and data breaches.
4. **Regulatory Engagement:** Engage with regulatory bodies to coordinate a proactive response and mitigate potential penalties.

This preliminary investigation brief provides an initial assessment of the situation, outlining the scope, initial evidence, and immediate concerns. As our investigation unfolds, we will continue to provide updates and recommendations to ensure the bank's swift recovery and compliance with regulatory requirements.

Signature:

Internal Audit Team, Finance Department