# Confidential Internal Memo

Project: Horizon Phoenix

Date: 14 August 2025

From: Jonathan Miller – Senior Security Analyst

To: Operations & Development Teams

## Subject: Security Vulnerability Report – URGENT

Following the penetration test completed on 13 August 2025, the following high-risk issues were identified in our production systems:

1. Customer Data Leak Risk:  
- Database server db-prod-03 contains an unsecured table with names, addresses, and credit card numbers for ~24,500 customers.  
- Vulnerability located in PaymentGatewayController.php line 221, related to unescaped SQL queries.  
- Impacted accounts include high-profile clients:  
 - Sarah Jenkins (CEO, J-Tech Solutions)  
 - Michael Zhang (CFO, BrightView Capital)  
 - David Ramirez (Minister of Infrastructure)

2. Hardcoded Credentials:  
- API key for Stripe payments: sk\_live\_51HvX34fL2mN7zQb6T...  
- Root admin password for staging server: Adm1n#2025! shared among three developers.

3. Network Exposure:  
- Firewall misconfiguration on vpn-hq-secure allowing inbound SSH from any IP.  
- Last successful suspicious login: 2025-08-12 02:14:55 UTC from IP 185.23.91.42 (Ukraine).

## Required Actions:

- Immediately rotate all credentials listed above.  
- Patch SQL injection vulnerability by end of day 15 August 2025.  
- Restrict VPN to internal IP ranges only.

Note: This memo and all attachments are classified INTERNAL – EYES ONLY. Any external sharing is prohibited and subject to disciplinary action.