lemnisk™

www.lemnisk.co

# 7 QUESTIONS FINANCIAL MARKETERS MUST CONSIDER TO EVALUATE VENDOR READINESS FOR DATA PRIVACY, SECURITY & COMPLIANCE

Financial marketers are under tremendous pressure to drive more revenue from digital channels. To pilot their digital presence, marketers engage technology vendors to craft customer journeys to increase engagement and conversions. While evaluating various vendors in the market, they often overlook the ability of the vendor to handle data security.

## Here are 7 crucial questions to consider while evaluating your vendor readiness for their data security, privacy & compliance.

### 1. SECURITY POLICIES

Are there comprehensive security policies in place at the leadership level to safeguard customer data?

### 2. INCIDENT MANAGEMENT & BUSINESS CONTINUITY MANAGEMENT

In the event of a security incident, are there appropriate management responsibilities and procedures in place?

### 3. ASSET MANAGEMENT

Has the customer data been classified in line with set expectations?

### 4. COMMUNICATION SECURITY

Do vendors have network controls & information transfer policies and procedures in place?

### 5. ACCESS CONTROL & CRYPTOGRAPHY

Is there an effective and proper use of cryptography employed for customer information protection?

### 6. 3rd PARTY VAPT

How frequently are vulnerability assessment & penetration tests run on their systems and are there any available reports?

### 7. COMPLIANCE

Have vendors achieved security compliance (ISO 27001:2013 & ISO 27018:2014)?

If your vendors do not have suitable responses to these critical data security questions, then in the event of a data security breach, marketers are equally responsible for lapses in data security. Your vendors should be accountable to the same data security standards the Financial Services industry would demand.