**Three Ways to Secure Mobile Banking Apps**

In recent times, it has become increasingly difficult for financial institutions to protect themselves and their customers from financial frauds and to safeguard their critical information. Introducing financial apps for customers is the need of the time, but at the same time increased cybercrimes have put users more at risk of losing their financial data through the use of mobile technology. More incidents of identity theft are now reported by customers than they were before, and this calls for the development of fully secure mobile applications that go through a thorough mobile app security testing process before they are accessible by customers.

In this environment of cyber insecurity, the reputation of mobile banking industry is at stake. According to a recent survey by Jumio, more than 75 percent millennials are not satisfied with their experience of mobile banking apps and term their main concern as security. Other than mobile app security testing, it is now time that financial institutions consider these important measures to build customer trust and loyalty.

**Multi-factor Authentication**

A simple password is not enough in today’s time to provide complete protection of an email or bank account. Just recently, Yahoo suffered a data breach resulting in more than 500 million accounts being exposed. If Yahoo had incorporated multifactor authentication, this breach could possibly have been avoided.

For mobile banking apps in particular, single verification is not enough. To ensure that customer data remains protected, they need to add an extra layer of security apart from password such as biometric recognition or facial recognition. Whether it is opening a new account or conducting a financial transaction, banks need to fulfill the “Know Your Customer” requirements through multi-factor authentication.

**Regulatory Compliance**

A robust strategy for mobile security requires compliance to security regulations. This not only enables organizations to adhere to best practices but also to avoid facing fines for noncompliance.

Regulations help banking organizations identify the identity of their clients and also prevent financial fraud, money laundering and identity theft.

**End-to-end Encryption**

Just like multi-factor authentication, end-to-end encryption is a much needed requirement for strengthening mobile security. When used along with mobile app security testing and security audits, end-to-end encryption ensures adherence to industry-specific standards and protection of data at both sending and receiving ends.

While banks provide convenience to customers through mobile banking apps to conduct quick online transactions, they also need to ensure that a good user experience does not come at the cost of their personal information being compromised.