MOBILE BANKING FOR THE FINANCIAL SERVICES INDUSTRY

MAY 2018 TECH BRIEF FOR THE FINANCIAL SERVICES INDUSTRY

The Mobile Transaction as the New Paradigm

Mobile banking has been defined as a service provided by banks, savings and loans, mortgage companies, and other financial institutions that will allow their clientele to initiate and complete financial transactions remotely and securely to bank branches, using a client-owned device, such as a personal computer, a PDA, a Smartphone, a tablet, or other such device. The device is used to connect to software through an installed application, or app, specifically created for this purpose, which is usually maintained and managed by the financial institution offering the mobile banking service.

With the widespread availability of devices and ease of use, how can Financial Services companies take maximum advantage of this burgeoning technology?

Labor Force Takeaway

Common use of personal digital devices (phones, tablets) is here to stay. Financial Services institutions would be well advised to embrace the proliferation of software and apps, incorporating new and tech savvy ways to engage their clients – and have their clients engage with them.

Deploying user friendly software for mobile apps and customer service should be on every business strategic plan. Further, the enhanced and expanded customer service helpdesk, available to assist clients who need support when interacting with these mobile apps, will be essential to ensuring clients feel their institution of choice is, in addition to being secure, friendly and easy to deal with. Certifications in helpdesk software, like ServiceNow, ZenDesk and ZoHo will give credibility and lend professionalism to this new workforce.

Customer service requirements will increase as the usage of new software is adopted. Technical Help Desk employees and Tier I and Tier II support titles, will need to be added to accommodate client needs as technology usage outside the company continues to rise.

Mobile Banking – The New Financial Paradigm

The client benefits of mobile banking are many. Clients can deposit, move, and withdraw funds conveniently without having to go to the financial institution. They can check balances, investigate rates, explore financial service offerings, and apply for loans any time of the day or night without involving the employees of the financial institution.

The trends in mobile banking adoption show no signs of abating. Consumers of financial services clearly have an appetite for mobile options, and financial services institutions are adding feature functionality to their systems as quickly as they feasibly can to meet user demand.

Users of financial services have mobile devices, and of those 43% had used mobile banking services in the past year, up from 39% the previous year. Of those users, 94% regularly check balances, 58% conduct money transfers, 56% receive text notifications of activity, and 48% use the check deposit scanning feature – all measurements up in double digits from the previous year's study (americanbanker.com).

With that said, utilization of in branch services remains active, suggesting that mobile services remain a complementary, not a full replacement service to, branch offerings. But the usage is strong and getting stronger, and banks are well served to continue to grow and expand on their mobile offerings.

Even non-financial services are jumping on the bandwagon. Companies like PayPal, Stash, Cash, Mint, and of course Amazon all have payment and cash movement apps that allow users to manage funds to vendors and other creditors outside of the traditional banking establishment. There are, however, issues that accompany this new found convenience of conducting financial transactions on the go.

In the area of security, consumers appear to be less confident about transaction safety as they have been since the inception of the Fed study. Confidence in the security of text messaging and app security overall hovers in the low 30th percentile, while the percentage of consumers who question the safety of apps in general is on the rise, close to 40% (americanbanker.com).

So the question becomes, if clients and financial institutions both want mobile banking, but security concerns plague usage, what can be done to mitigate risk so both users are happy?

It's first important to define the ecosystem in which these transactions occur, in order to determine where the security concerns may exist. For example, security concerns exist at each transactional stage – at the PDA, within the app, in accessing or the internet, and in connecting with the bank legacy system. The bank, or financial institution, can only control the security at the points within their control, that is, the app for which they have contracted, and the legacy system authentication (entry) point.

Security issues at the app end can basically be combined into two categories, Personal Identification Integrity (typically a function of firmware and software) and Message Integrity (usually compromised by malware and virus attacks). These items are best controlled through strong authentication policies. Other measures to control include Access Control include idle time screen lockout, and strong passwords; Application Provenance (identification of author so user can decide if safe); Encryption; Isolation (typically used for highly sensitive data);

and Permissions-Based Access Control.

At the legacy systems end, the security issues are generally limited to access methods – hacking, and authentication – which are handled by firewalling at the server end. They are not similar to the mobile device security issues, but obviously can be equally lethal.

These issues are typically managed by the financial institutions IT team, either in house or outsource, and involve a healthy mix of process, policy, devices, and monitoring to achieve true security compliance.