Access Control in Banking:

IMPROVING SECURITY WITH BIOMETRICS

- By Afiq Jauhari, Marketing Executive cum Copywriter, FingerTec Worldwide

IN December 2011, the five largest banks' (JPMorgan Chase, Bank of America, Citigroup, Wells Fargo and Goldman Sachs) assets in the United States of America equaled 56 percent of the U.S. economy as compared with 43 percent from 2006 (Fatima, 2011).

The industry's growth over the time period is a strong indicator that banking in the nation has bounced back favorably from the recent economic crisis a few years ago. Moving away from the economic climate concerns, most physical retail banks are now facing issues with access control brought on by technological advancement, both in terms of satisfying customer expectations by providing high-tech solutions and ambience, as well as securely safeguarding their assets and premises.

This article addresses these two main concerns of the banking industry when dealing with their customers and employees, in addition to taking a look at how FingerTec solutions, particularly biometric devices, can help solve these issues.

Issues In Managing Physical Banks

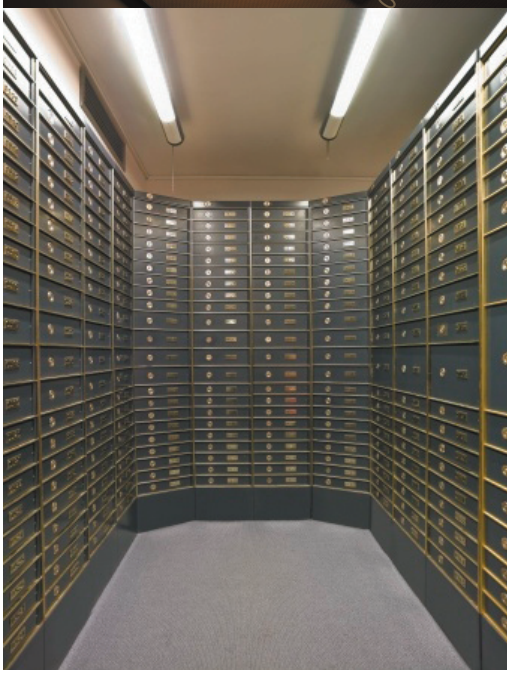
As discussed in the previous section, customer satisfaction in terms of security is a major concern in the banking industry, especially as it is providing services that require actual face-to-face interaction between its staff and employees at the bank. In recent years, the expectations of the general public has increased in terms of the security they are entitled to and this has challenged the physical banking industry to provide improved services, not just in terms of the staff's treatment of customers. This also includes the technologies employed in the banks themselves to reassure customers of its safety (Jain, Hong, & Pankanti, 2000). However, this is much easier said than done, as there are many hurdles to overcome by the management and industry at large.

Firstly, customers need to be able to trust that others cannot access their deposits. This can happen if the verification methods used by banks are inadequate. There are basically two points of interaction whereby a bank's patron is required to verify himself, which are during over-the-counter transactions (such as putting in deposits or applying for loans) and use-of-facility transaction (such as automated teller machines or safety deposit boxes). As such, identity fraud has been a thorn in banking's side as the verification process needed before performing a transaction usually only requires minimal documentation or a signature. This exposes the bank to risk of forgery, which in turn will cause them to lose not only their assets but also the trust of their customers (Khan, Khan, & Alghathbar, 2010).

However, as some banks have become more stringent with their verification methods to curb forgery, this has instead caused some customers to feel a bit of a hassle. This is due to them having to provide different types of identification credentials for transactions that may have been simpler previously. Although the transactions are more secure, they are unfortunately less user-friendly and require more time and effort on the customer's side. Combined with the previous issue of forgery, it is thus of utmost importance to provide customer satisfaction by finding the right verification method to employ in the said banks.

On top of the issues surrounding identity verification, another aspect that needs to be examined for banks is their actual physical security. Safeguarding the premises, both during working hours and off it, is integral in maintaining the safety of not only the actual bank but also of its assets and working documentations (Liu & Silverman, 2001). This is made complicated by the different levels of access required by different employees into separate areas of the bank. For example, an hour before the bank opens, the branch manager and two other employees are given access into the safe but only the branch manager is given access once the bank opens.

In addition to these issues surrounding the banking industry; mainly raising customer satisfaction through secure verification methods and safeguarding physical access, there are also other concerns regarding access control that not only affects the banking industry but most other industries as well. However, only the issues previously discussed will be explored further in the next section to exemplify how biometrics technology, particularly solutions from FingerTec Worldwide, can aid them.



Banking on Biometrics

Among the significant concerns discussed in the previous section, all of them can be eliminated or improved upon with the help of current technological advancements. This is possible because of a plethora of already existing tools that can provide relief from the troubles faced in the banking industry, among them being biometric devices. These devices are used to assist in verifying one's identity using a unique attribute already on the user such as via fingerprint or facial recognition. The usage of these devices*, as well as a proper access control management software can enable the banks to face and solve these conundrums (Yang, 1997).

Firstly, biometrics can help reassure customers of the safety standards used in banks by using it to eliminate identity fraud. As every major transaction is preceded by a verification method to identify a bank customer, combining biometrics in the process will undoubtedly eradicate forgery as every fingerprint is uniquely attributed to a single person. This will not only restrict fraudulent transactions and save the bank from losing its funds, but also to display the level of security employed by the bank to its customers. This can be achieved by installing FingerTec OFIS-Y, a high quality USB plug-and-play fingerprint reader, as the verification method for certain transactions.

Other than jettisoning identity fraud from the picture, biometric devices such as FingerTec OFIS-Y can also help improve on user experience because of its speed and accuracy. This is due to the fact that the biometric device is able to capture a fingerprint image, then cross-check with its existing database (either locally or online) and verify a person within mere seconds, eliminating a large chunk of the waiting time. Making this scenario possible is the latest VX10.0 algorithm used in the technology, which also ensures that important fingerprint information cannot be stolen and duplicated.

On top of achieving customer satisfaction by eliminating identity fraud and improving user experience, biometrics can also be used to implement an advanced yet easy-to-use access control system to safeguard the premises as well as restrict access into different areas of the bank. By combining a biometric device, such as FingerTec R2, with a proper access control management application, such as Ingress, even complicated implementations can be set up easily. This is made possible with the Time Zone settings in Ingress, which enables administrators to decide differing levels of access for staff according to their policies.

In conclusion, the issues that are facing physical banks, such as satisfying customer expectations by providing high-tech solutions and ambience as well as securely safeguarding their assets and premises, can all be improved and handled with the correct implementation of an advanced or simple access control system using biometrics technology.

**Biometrics solutions from FingerTec are used to demonstrate how the technology can help solve these issues*

Higher Efficiency via Biometrics

At the end of the day, implementing an access control system using biometrics will require a high level of commitment from the banks. However, the long term benefits gained from such an implementation is gargantuan as compared to the miniscule hassles involved early on. Not only will it be able to improve customer satisfaction and the premises' security, but it can also reduce the time and effort previously spent on traditional verification or locking methods. This will ultimately result in higher efficiency.

As the banking industry continues to tread water in the future, efficiency is king when it comes to business growth. Having a reliable access control system such as the one from FingerTec Worldwide can definitely contribute to the cause and definitely outweighs the initial costs of implementation. However, cooperation from all staff as well as support from the service provider early on in the process is integral for the successful deployment of any systems.

Bibliography

- **Fatima, A. (2011, August).** *E-Banking Security Issues.* Is There A Solution in Biometrics? . Journal of Internet Banking and Commerce , 13-16.
- **Khan, B., Khan, M., & Alghathbar, K. (2010, November).** Biometrics and identity management for homeland security applications in Saudi Arabia . African Journal of Business Management , 3296-3306.
- **Liu, S., & Silverman, M. (2001, January).** A practical guide to biometric security technology. IT Professional , 27-32.
- **Jain, A., Hong, L., & Pankanti, S. (2000, February 25).** Biometrics: Promising frontiers for emerging identification market . Retrieved January 16, 2014, from Penn State University Online Literature: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=?doi=10.1.1.10.5497.
- **Yang, Y. (1997).** *The Security of Electronic Banking. Proc. Nat. I International Systems Security Conference , 41-52.*

www.fingertec.com