

International Market Trend: Online Banking Identity Checks Still Unregulated Under Egyptian Laws

Rana Hegazi - Senior Associate - Corporate / Mergers and Acquisitions
r.hegazi@tamimi.com - Kuwait City

November 2016

Several banks operating in Egypt are currently introducing mobile banking applications with the desire to benefit from the widespread present use of technological tools such as smart phones and social media platforms. Such electronic mobile payment systems are expected to increase the competition among banks to offer applications which meet consumers' needs. Egyptian laws do not currently provide specific regulations regarding the complex new electronic identity verification methods and solutions (eg. fingerprints and facial recognition solutions). Nevertheless, mobile payment services and processes are generally regulated by circulars issued by the Central Bank of Egypt (the "CBE") that will apply indirectly to all queries regarding electronic mobile payments and identity verification solutions. This article will shed light on the most important compliance obligations to be followed by such solutions service providers.

Mobile Payments Subject to General System Security and Data Protection Obligations

The board of Directors of the CBE issued a Decision dated 2 February 2010 providing for the regulations regarding the operation of mobile payment services in Egypt (the "Decision"). The Decision requires the issuing bank to ensure proper identification of the system's customers and proper authorisation to access the system.

Additionally, pursuant to the Decision dated 14 April 2011 issued by the Anti-Money Laundering Unit, the issuing bank must ensure that electronic payments comply with Anti-Money Laundering Authority measures for proper identification of customers and service providers. A list of necessary documents and information is required to be submitted by each customer. The issuing bank should establish policies and procedures to protect the system's security in addition to protecting the integrity and confidentiality of the customers' data as per Article 100 of the Banking Law (Law No. 88 of 2003) which regulates the confidentiality of client and account information.

Consistent with this, if the bank has direct or indirect access to its customers', clients', suppliers' or distributors' account information and banking details, it must maintain the strict confidentiality of the same and refrain from any disclosure or transfer of such information. Therefore, any mobile payment service provider must ensure it has customer approval for such transfer of data before undertaking its function.

Addressing the Absence of Regulatory Compliance Obligations

As mentioned above, there are no specific regulations regarding such mobile payment service providers. However, electronic signatures and electronic documents are legally recognised by the Organisation of E-Signatures and establishment of the Information Technology Industry Development Agency Law issued by Law No. 14 of 2005, hereinafter referred to as the "E-Signature Law" and its Executive Regulations issued by the Ministerial Decision No. 109 of 2005 (the "Executive Regulations"). In fact, Articles 14 and 15 of the E-Signature Law state that, within the scope of civil, commercial and administrative transactions, E-

signatures, E-documents and electronically written messages shall have the same force and determinative effect that signatures, documents and official / unofficial messages have under the provisions of the Evidence Law in Civil and Commercial matters (Law No. 25 of 1968). Moreover, Article 1 of the E-Signature Law defines 'Electronic Writing' as 'all the letters, digits, symbols or any other signs on an electronic, digital, photographic support or any other similar means that gives perceptible indication' and defines an E-signature as 'an electronically written message in the form of letters, digits, codes, signals or others and has a unique identity that identifies the signer and uniquely distinguishes him/her from others'. Such a broad definition may encompass mobile payment service providers. Therefore, these electronic authentication methods would be considered legal and applicable in Egypt.

Having said that, the Decision provides that the issuing bank and the service provider must ensure the highest security standards of encryption and authentication of originator identity. Additionally, a double authentication access process must be in place, using phone numbers and PIN to originate a payment instruction. It is to be noted that the Decision stipulates that PINs must satisfy certain requirements. For example, PINs must be composed of a minimum of 4 digits (preferably 6) and must not appear as readable text on any system computer during the process. The Decision also provides that when a payment system is accessed by internet through web protocols from a mobile phone and the phone number cannot be verified, the identity verification must include a name and a password of not less than 8 digits in addition to the PIN of the service.

Security Requirements

Even though the CBE did not yet issue yet a regulation regarding the mobile payment service providers, the Decision issued by the Executive Director of the Anti-Money Laundering Unit dated 14 April 2011 provides that a periodical risk analysis of the system should be undertaken, including conducting penetration tests and ethical hacking to ensure the strength of the system. Additionally, according to this Decision and the CBE's regulations, the IT structure operating the mobile and internet banking must include firewalls, intruder detection systems, data file and system integrity checking, as well as surveillance and incident response procedures.

Strict procedures should also be applied for the physical security of access to programmes, networks, and any equipment operating mobile payment solutions. Strict protection of system encoding keys should be ensured.

It is to be noted that the CBE is entitled to supervise any part of the system to make sure it complies with its measures and specifications.

Consumer Protection Obligations

According to CBE regulations, mobile payment service providers must set up maximum limits for daily and monthly withdrawal operations. This will depend on the amount of risk related to the service and the risk management reports submitted by the Bank related to the service.

In the event of disputed transactions or system customer complaints, the dispute resolution must be subject to fixed rules announced to the customers. These rules must be stated in the agreement entered into between the customer and the bank. This agreement shall stipulate the customer's responsibilities to keep his pin code secure and to immediately report the loss of his mobile phone as well as the reimbursement conditions, if any, and any service charges or fees. A form of these conditions must also be published on the bank's website.

Conclusion

At present, the Egyptian government has a policy at a national level of encouraging electronic payments to increase efficiency and transparency. The financial significance of this was marked on 3 March 2015 by the announcement of a partnership between Egypt and MasterCard to extend e-financial services to 54 million

Egyptians. Part of this development will be by rolling out a digital ID program that links Egyptian citizens' national ID to the existing national mobile money platform.

The CBE regulations need to be amended and updated in order to face the emergence of e-financing in Egypt. Whilst the E-signature Law does cover mobile payment service providers, legislation specifically tackling electronic banking and financial operations is needed and should be brought forward. Such legislation should also prevent and protect electronic payments customers from technical issues, the absence of regulation hitherto having been bridged by some of the CBE's circulars and data protection provisions.