Central Bank of Oman

البنك المركزي العماني

Circular BM - 1136

June 16., 2015

To: All Licensed Banks operating in the Sultanate of Oman

After Compliments,

Subject: Security of Electronic Banking Systems

Central Bank of Oman has been alerting banks from time to time with regard to safety and security of all electronic banking channels, including online banking/ Internet banking, phone/ mobile banking, cards and POS systems. As the use of electronic banking channels for banking transactions have become more widespread, security of the systems used by the banks for the purpose has assumed increased critical importance.

2. 'Risk Management Principles for Electronic Banking' published by the Basel Committee on Banking Supervision in July 2003 had laid down the risk management principles for electronic banking. These principles are listed in Annexure-1 for ready reference. These principles have been categorised broadly under Board and Management Oversight (*Principles 1-3*), Security controls (*Principles 4-10*) and Legal and Reputational Risk Management (*Principles 11-14*). Banks should also pay special attention to the sound practices in respect of security control practices, managing outsourced systems, authorisation for e-banking applications, audit trail practices, maintaining customer privacy, business continuity and contingency for e-banking, as set out in the appendixes to the Basel paper.

3. As banks are aware, electronic banking systems in general and online banking systems in particular have also become a prime target for fraudulent attacks, which call for increased attention to related security controls. The target of a fraudster/ hacker, leading to a compromise of the system, could be one or more of the following components in respect of online banking:

i) the Internet banking server
ii) the communication channel
iii) the user terminal/ user

A brief explanation of the above generic categories of possible attacks is given in Annexure-2. Similar attacks could be targeted at other channels of electronic banking as well.

4. The nature of such attacks directed against the electronic banking systems of banks and/ or their vendors, systems used by the merchant outlets and customers, and networking/ communication channels by exploiting the inherent weaknesses

have become diversified and the attacks are also increasing in degree of complexity, innovation and sophistication over a period of time. Central Bank has noted that banks have adopted various countermeasures including: ensuring that customers use strong passwords, providing virtual keyboards for entering login passwords, Secure Sockets Layer (SSL) encryption, sending customers information on how to avoid falling prey to malicious attackers and implementing two-factor authentication. Banks are advised to strengthen their technical, operational and security framework to meet the challenges to the security of the electronic banking systems.

5. Based on the past instances of attempted frauds on electronic banking systems, as also the examination findings on IT security and controls related to electronic banking, some of the aspects to which banks need to pay particular attention are listed below. Banks are, however, advised to note that the measures suggested below are not exhaustive and that they need to proactively take such other measures as appropriate from time to time to ensure the security of banking systems.

a) Banks should put in place robust security architecture with a defence-in-depth strategy to strengthen their security framework. The security at each layer should further be enhanced by segmentation of the LANs, deployment of firewalls/ intrusion prevention and detection systems, etc. and by taking such other measures as deemed suitable and appropriate to the security architecture.

b) Local banks should set up Information Security Departments (ISD) with adequate and appropriate manpower resources and entrust the ISD with responsibilities of guarding the IT infrastructure, systems and information of the bank. Further, banks shall conduct ongoing review on the adequacy and appropriateness of technology and infrastructure deployed for electronic banking services to guard against possible/ emerging security threats. Cost should not be a consideration for the same. Branches of foreign banks should also have an appropriate organisational framework for information security, consistent with the size and scale of operations in the Sultanate.

c) Banks need to define Minimum Security Baseline (MSB) standards for all the delivery channels, systems, equipment and networks, which should be supplemented with periodic checks by the security teams for compliance to these baseline standards. Security teams need to refresh the MSBs and the rules configured in automated log monitoring systems periodically in the light of emergence of new threats and vulnerabilities and experience gained.

d) Formal incident reporting and management procedures should be put in place to handle any suspicious and unusual transactions that are detected. Banks should also strengthen the alerting and warning systems in the security architecture to detect and report suspicious and unusual activities. For this purpose, banks need to enable generation of logs for all the delivery channels, systems, databases and networking equipment. These logs should be subjected to continuous monitoring by the security teams by deploying independent automated log monitoring systems.

e) Banks should have a robust and effective automated fraud monitoring mechanism in place to detect, in a timely manner, suspicious transactions and unusual activities based on predefined rules and criteria *(e.g. transactions initiated from an Internet Protocol (IP) address different from the one usually used by the customer, fund transfers which have not been done before or fund transfers of amount up to the maximum allowable transaction limit of the customer account*).

f) Even a minor security loophole can provide room for a cyber-attack/ perpetration of fraud on banking systems. Therefore, banks need to conduct Vulnerability Assessment and Penetration Testing (VAPT) to detect the vulnerabilities if any and to take remedial measures. VAPT should be carried out at least on quarterly basis by internal security teams and at least once in a year by external experts.

g) Wherever banks have outsourced (with necessary prior approval of CBO as required under Circular No. BM-1080 dated April 16, 2011) any of the processes of electronic banking or information security related activities, they shall, through due diligence, binding agreements (with appropriate liability clauses) and adequate ongoing oversight, ensure that the systems and procedures at the third party vendor level are adequate and do not pose any security threat to the electronic banking systems of the bank.

h) Banks shall also put in place adequate risk mitigants like clarity on mutual roles and responsibilities, indemnities, independent audit and control, apart from obtaining insurance against security related frauds and cyber threats. Further, wherever third parties are associated with any of the electronic banking activities, banks shall bind the third parties with liability clauses in respect of any security threat impacting the bank's systems that emanates from the third party's system.

i) As part of anti-fraud measures, banks should notify the customers using SMS alerts and email messages on all financial and non-financial transactions (*notably change of contact details, ATM pin change, e-banking login and failed attempts, failed/declined transactions, etc.*).

j) As human interface is often perceived as one of the weakest links in the information security chain, banks are advised to take steps to promote security awareness on cyber frauds notably 'phishing' and 'vishing' attacks to the customers, vendors and employees through awareness sessions, emails, SMS and advisories on ATM/CDM screens and corporate website.

k) Banks should pay special attention to the provision of easy-to-understand and prominent advice to customers on Internet banking precautions, in particular, advising the customers to ensure that their computers/ mobile devices are securely configured and that they are adequately protected from computer viruses and malicious programs. Customers should be reminded to provide a

valid mobile phone and contact numbers for notification purpose and notify the bank timely if any of these numbers are changed.

l) Robustness in IT security cannot be considered in isolation. One related failure has been lack of communication between banks and their customers and staff. The importance of awareness and alertness, including a list of do's and don'ts, should be emphasized on a regular basis.

m) Further, the information security department/ units should explore conducting mock cyber-attack drills under real-life circumstances involving scenarios such as phishing emails and to use such tests for gauging the security awareness of employees.

6. Wherever banks take up new electronic banking initiatives, capacity building and preparedness should be ensured in the context of all risk dimensions. Further, it is an acknowledged fact that fraudsters, particularly in relation to information technology, try to keep ahead of the service providers. Therefore, there is a need for commensurate proactive, preventive and follow-up vigilance and actions on the part of banks and their service providers.

7. It has also been the experience that the types of frauds/ malpractices that are observed in one jurisdiction tend to get perpetrated in other jurisdictions at a later date. Therefore, banks also need to keep themselves abreast of global developments in respect of bank-related frauds/ cyber-attacks and their modus operandi which had been detected/ occurred in other countries also. Banks should review the controls within their systems in the light of those frauds/ cyber-attacks for taking suitable remedial steps to prevent/ avoid the occurrence of similar frauds.

8. It is reiterated that banks are required to keep CBO and ROP informed of any instances of attempted frauds and frauds detected within the time schedule given in para 3 of Circular no. BM 1078 dated 18.01.2011.

Best regards,

Hamood Sangour Al Zadjali
The Executive President

Encl: as stated

(Annexure-1 to Circular BM 1136 dated 16/6/2015)

Risk Management Principles for Electronic Banking:

The Principles set out in the document "Risk Management Principles for Electronic Banking" (*http://www.bis.org/publ/bcbs98.htm*) issued by the Basel Committee on Banking Supervision (BCBS) are listed below and set the minimum requirements to be complied by the banks in establishing their policies and processes for e-banking.

Principles 1-3: Board and Management Oversight:	
Principle 1	*The Board of Directors and senior management should establish effective management oversight over the risks associated with e-banking activities, including the establishment of specific accountability, policies and controls to manage these risks.*
Principle 2:	*The Board of Directors and senior management should review and approve the key aspects of the bank's security control process.*
Principle 3:	*The Board of Directors and senior management should establish a comprehensive and ongoing due diligence and oversight process for managing the bank's outsourcing relationships and other third-party dependencies supporting e-banking.*
Principles 4-10: Security Controls:	
Principle 4:	*Banks should take appropriate measures to authenticate the identity and authorisation of customers with whom it conducts business over the Internet.*
Principle 5:	*Banks should use transaction authentication methods that promote non-repudiation and establish accountability for e-banking transactions.*
Principle 6:	*Banks should ensure that appropriate measures are in place to promote adequate segregation of duties within e-banking systems, databases and applications.*
Principle 7:	*Banks should ensure that proper authorisation controls and access privileges are in place for e-banking systems, databases and applications.*
Principle 8:	*Banks should ensure that appropriate measures are in place to protect the data integrity of e-banking transactions, records and information.*
Principle 9:	*Banks should ensure that clear audit trails exist for all e-banking transactions.*
Principle 10:	*Banks should take appropriate measures to preserve the confidentiality of key e-banking information. Measures taken to preserve confidentiality should be commensurate with the sensitivity of the*

	information being transmitted and/or stored in databases.
Principles 11-14: Legal and Reputational Risk Management:	
Principle 11:	*Banks should ensure that adequate information is provided on their websites to allow potential customers to make an informed conclusion about the bank's identity and regulatory status prior to entering into e-banking transactions.*
Principle 12:	*Banks should take appropriate measures to ensure adherence to customer privacy requirements applicable to the jurisdictions to which the bank is providing e-banking products and services.*
Principle 13:	*Banks should have effective capacity, business continuity and contingency planning processes to help ensure the availability of e-banking systems and services.*
Principle 14:	*Banks should develop appropriate incident response plans to manage, contain and minimise problems arising from unexpected events, including internal and external attacks, which may hamper the provision of e-banking systems and services.*

(Annexure-2 to Circular BM 1136 dated 16/6/2015)

Types of Internet Banking Attacks

To categorize Internet banking attacks, each component of the process should be examined:

- the Internet banking server (IBS).
- the communication channel (CC) and
- the user terminal/user (UT/U),

IBS attacks - These types of attacks are offline attacks against the servers that host the Internet banking application. Examples include:

1. Brute-force attacks - Brute-force attacks in certain password-based mechanisms are reported to be feasible by sending random usernames and passwords. The attacked mechanisms implement a scheme based on guessable usernames and four-digit passwords. The attack mechanism is based on distributed zombie personal computers, hosting automated programs for username-based or password-based calculation. This attack may be combined with username filtering methods for determining the identity of the user. These methods filter the different responses of the server, in the case of valid or invalid usernames.
2. Bank security policy violation - Violating the bank's security policy in combination with weak access control and logging mechanisms, an employee may cause an internal security incident and expose a customer's account.
3. Web site manipulation - Exploiting the vulnerabilities of the Internet banking web server may permit the alteration of its contents, such as the links to the Internet banking login page. This may redirect the user to a fraudulent web site where his/ her credentials may be captured.

CC attacks - This type of attack focuses on communication links. Examples include:

1. Pharming - These involve compromising domain name servers (DNSs), altering DNS tables and connecting the user to fraudulent sites, instead of the official bank's site, where information regarding the user's account may be derived.
2. Sniffing - Active sniffing attacks masquerade the two communicating entities to each other (user client and the Internet banking server) to capture information, such as username and password. Passive sniffing captures information from the communication medium, without interception.
3. Active man-in-the-middle attacks - This type of attack regards a schema where the attacker receives and forwards information between the UT and the IBS. The attacker sends malformed user packets or injects new traffic, such as transfer commands, from one account to another.
4. Session hijacking - Attacks that force the user to connect to the IBS with a preset session ID. Once the user authenticates to the server, the attacker may utilize the known session ID to send packets to the IBS, spoofing the user's identity.

UT/U attacks - These attacks target the user equipment, including the tokens that may be involved, such as smartcards or other password generators, as well as the actions of the user. UT/U attacks include:

1. Procedural attacks:
   - User surveillance (piggybacking) - Similar to the personal identification number (PIN) thefts facilitated by the installation of cameras in automatic teller machines (ATMs); the user's actions may be monitored to capture credentials.
   - Theft of token and handwritten note stealing - Internet banking usernames are usually long and have to be written down. Users may also keep their passwords written, despite the security guidance provided by their banks. Notes may be stolen, providing access to the user's credentials. Tokens may also be stolen, providing the attacker with one authentication factor that, when combined with other types of attacks (such as PIN calculators), can lead to identity theft.
2. Malicious software installation. The embedding of malicious content for compromising the user's login information and password (e.g., keyboard loggers or screen capture in image or video files) may take place via a number of different methods, including:
   - Hidden code - This is the use of hidden code within a web page that exploits a known vulnerability of the customer's web browser and installs malicious software in the user terminal. The exploit may target permissions on Java runtime support, ActiveX support, multimedia extensions, and automated download and running of software through the browser.
   - Worms and bots - Worms search vulnerabilities and exploit them automatically. This includes the exploit of instant messaging and chatting communication software (that allows the embedment of dynamic content), which may automatically be deployed using bots.
   - E-mails with malicious code - This is the submission of e-mails with malicious content, such as executable files or HTML code with embedded applets.
3. Token attack tools:
   - Smartcard analyzers - Attacks against smartcards, such as power consumption analysis or time analysis, may expose the security of the smartcard by revealing cryptographic keys and passwords.9 Such attacks are sophisticated and not easy to implement, but are very effective, especially if the necessary countermeasures (noise generators, time-neutral code design) against these types of attacks are not implemented by the smartcard manufacturer.
   - Smartcard reader manipulator - This is applicable to noncertified smartcard readers with insecure interfaces, which may expose the contents of the smartcard by conducting unauthorized operations.

- Brute-force attacks with PIN calculators - These attacks focus on breaking the security of tokens that generate random PINs. The attack exploits the fact that a time window is necessary, for synchronization reasons. In some implementations, except from the present PIN, the subsequent and preceding codes are active for the same purpose. It is reported that it is possible to break such mechanisms with a minimum window of three PINs.

4. Phishing. These attacks use social engineering techniques - masquerading as a trustworthy person or business in an electronic communication - in an attempt to fraudulently acquire sensitive information, such as passwords and credit card details. These attacks include:

- Social engineering - These attacks focus on the compromise of the user's credentials by nontechnical means, such as phone calls or the submission of e-mails masquerading as an official bank, asking the user for username and password.
- Web page obfuscation - These attacks are based on links that do not correspond to the destination they describe, or the use of Internet Protocol (IP) addresses instead of universal resource locators (URL) for confusing the user. Other techniques deploy hidden frames. These are used for covering the real activity of a web page by using several frames with malicious content, while the user sees only the URL of the master frame set. Other methods use graphics that spoof the interface of a web browser, such as the address bar.

Ref: A paper on 'Analysing the Security of Internet Banking Authorisation Mechanisms' published in the Information Systems Control Journal, Volume 3, 2007.