BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Telephone 60(3) 2698 8044 Jalan Dato' Onn
Facsimile 60(3) 2697 0086 50480 Kuala Lumpur
Web www.bnm.gov.my Malaysia

SULIT

Our Reference: C8R2016-0155

21 Julai 2016

Rahsia Besar	Rahsia	Sulit	Terhad	Umum

PENYELIAAN	1st Level	2nd Level
Date Received	5th July 16	21/7
Assigned to	[redacted]	[redacted]
Date line		

Remarks
Need to closely work w/ IT team to ensure fully comply w/ required timeline

Ketua Pegawai Eksekutif

Ground Floor, East Block
Wisma Selangor Dredging
142-B Jalan Ampang
50450 Kuala Lumpur

Tuan,

Security Controls for Internet and Mobile Banking

As we strive for a higher adoption and acceptance of online banking channels by customers via Internet and mobile banking, cyber threats and fraudulent scams continue to pose major risks to the financial industry. Such challenges, if not properly managed, can undermine the confidence of the public on the Internet and mobile banking as an alternative secure and safe channel for conducting banking transactions. In this regard, it is critical for Financial Institutions (FIs) to strengthen their controls and processes in mitigating these risks, in pursuit of promoting e-payment strategies.

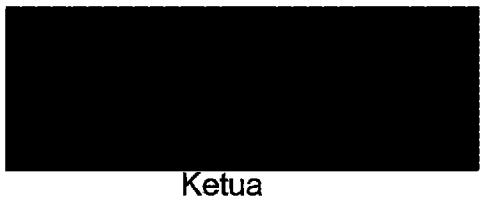
2. In particular, we note some FIs have increased the daily open funds transfer and bill payment limits without ensuring adequate security controls are in place to mitigate risks involved in the Internet and mobile banking. Consequently, these FIs become targets to cyber criminals and fraudsters due to the appeal of obtaining large sums of money through a one-time attack on a real-time basis. These cyber criminals and fraudsters usually prey on unwary customers that have low awareness on information security. Hence, FIs are required to put in place at minimum, security controls as outlined in **Appendix 1**. All the risk management controls outlined are applicable for open funds transfer for the Internet and mobile banking services provided for individual well as for where appropriate. [redacted] is required to review and assess level of comp w appropriate undertake remedial measures to address any gaps.

3. We are cognisant that security controls for the Internet and mobile banking will continuously evolve in line with emergence of new threats and innovations. Therefore, **Appendix 1** should not be taken as an exhaustive list. Going forward, [redacted] i is expected to continuously assess the effectiveness of these security controls. Finally, [redacted] is strongly urged to continue promoting security awareness programmes for its customers so that they are informed of the latest developments and requirements for secure online banking transactions and remain vigilant to cyber threats and fraudulent scams.

4. Should you have any queries relating to the content of this supervisory letter, please contact

Sekian, harap maklum.

Yang benar,



Ketua
Unit Pakar Risiko

s.k. Pengarah, Jabatan Penyeliaan Perbankan

Appendix 1

Minimum Requirements on Security Controls for Internet and Mobile Banking Services

No.	Security Requirement	Timeline
(a)	Provide transaction details in all Short Messaging Service (SMS) notifications including during generation of Transaction Authentication Code (TAC) or One-Time Password (OTP) (e.g. beneficiary's name as registered under the account, transaction amount, date and time).	3 months
(b)	Require TAC or OTP when registering an account as a "favourite" beneficiary. Require a different TAC or OTP for the first time funds transfer to the "favourite" beneficiary.	3 months
(c)	For new Internet banking customers, the default transfer limit to third parties must not be more than RM5,000 per day. Adopt lower default daily limit for open funds transfers via mobile banking. Provide capability for customers to change the transaction limit via secured channels (for e.g. online with two-factor authentication or at the branch premises).	3 months
(d)	Implement image or word verification authentication to enable customers to identify the FI's genuine website. The system should require the customer to acknowledge that the image or word is correct before the password box is displayed to the customer.	6 months
(e)	Deploy automated fraud detection system which has the capability to conduct heuristic behavioural analysis.	12 months
(f)	Mobile banking application must run on secured versions of operating systems only and must be able to detect and block application from jail broken and rooted devices.	3 months

(g)	FIs using SMS TAC as the second factor authentication (2FA) for Internet banking are required to implement alternative and stronger two-factor authentication (2FA) solutions for funds transfers and bill payment to third party transactions above RM10,000 with the following features: • Ability to bind the device's unique number to the customer's account if using devices to generate a OTP (e.g. device ID such as IMEI, exchange of digital certificates); • Ability to bind the transaction details to the OTP generated by the device (e.g. beneficiary account number, amount of transaction); • Generation of the OTP at the device must be initiated from the customer's device and not from the bank's server; and • OTP must always be encrypted and not stored anywhere. However, FIs that have yet to put in place a stronger 2FA may continue using SMS TAC for high value transactions (above RM10,000) for its existing and new customers until the stronger 2FA is implemented.	24 months