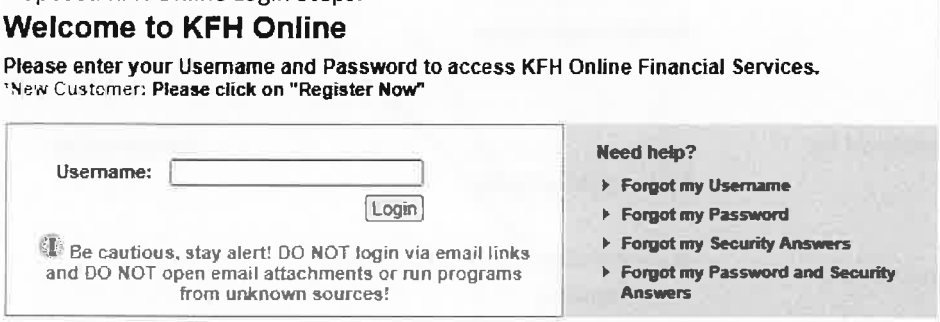
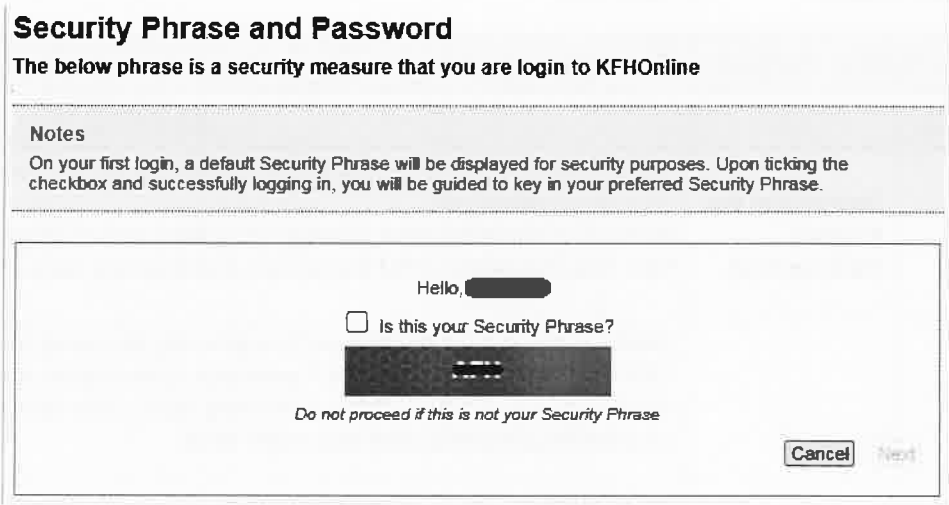
BUSINESS REQUIREMENTS – Strengthening Measures to Mitigate Fraud through Phishing of SMS One Time Password (OTP)

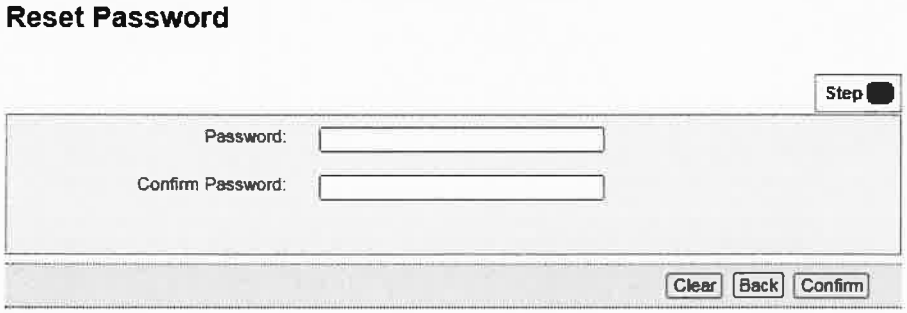
REQUESTOR DETAIL

Requested by	Abidah Faqih Haron		
Reviewed by	Malarvili Muniandy	**Concurred by**	Gary Oh Chee Ming
Department	eChannels Developments & Cards, Retail Banking.		
Date Request	01 June 2020		

BUSINESS REQUIREMENT DESCRIPTION

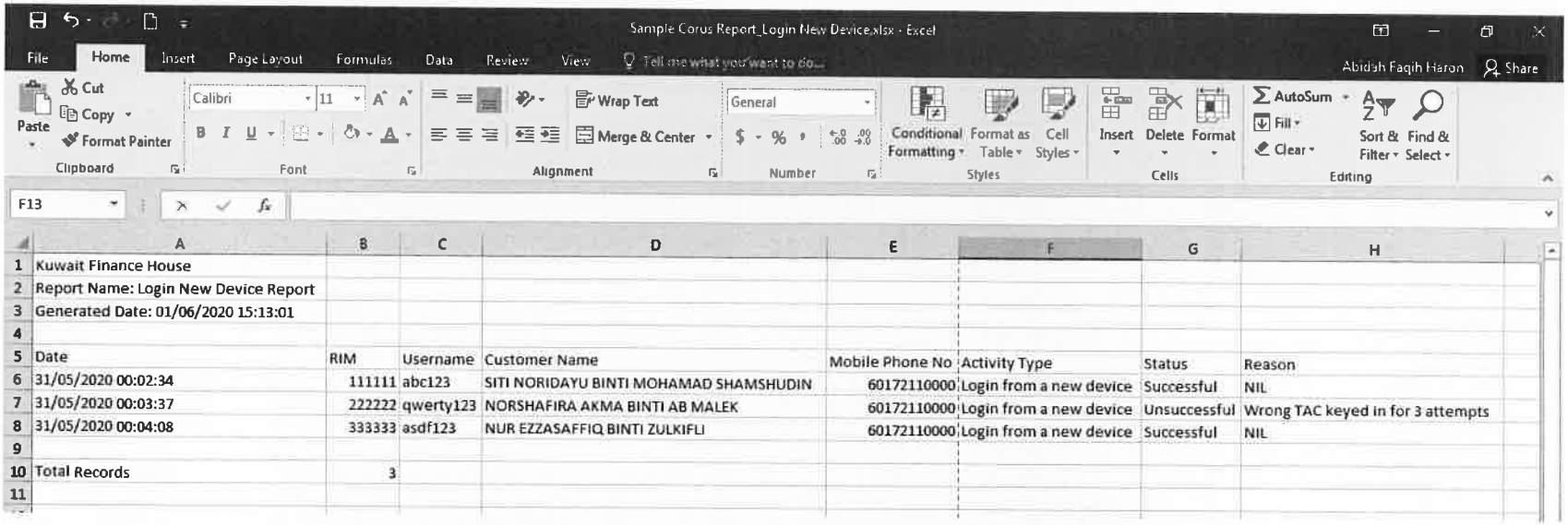
NO	ITEM	DESCRIPTION
1.	**Objective of the Project / Enhancement**	The enhancement is to comply with the BNM requirement which is to address the SMS OTP/TAC fraud more effectively. Referred to the BNM letter: Strengthening Measures to Mitigate Fraud through Phishing of SMS One Time Password (OTP)/ Transaction Authorisation Code (TAC) dated 15 April 2019.
2.	**General Overview**	BNM has issued a Notification on Strengthening Measures to Mitigate Fraud through Phishing of SMS One Time Password (OTP)/ Transaction Authorisation Code (TAC) dated 15 April 2019 rising concern on the number of internet banking fraud cases related to compromise of SMS/TAC increased significantly since September 2018. Assessment on the effectiveness of the control to mitigate SMS OTP/TAC fraud risks has been done by the Internal Audit. Based on the summary Internal Audit report dated 13 May 2019 there are 2 gaps that need to be addressed: 1. Inability of the Internet Banking (IB) system to identify an account being activated using a different customer. a. On the current measures control, there is no SMS alert or notification to the customer when log in into new/different devices. The IB ystem does not have the capability to alert customer when account is being activated using different device. b. The enhancement is required where the SMS alert or TAC will be sent to customer when an IB account is being activated using a different device. 2. Alphanumeric password to access internet banking account has yet to be enforced. c. On the current measures control, the password combination requires of alphabets, numbers and symbols without enforcement. d. The enhancement is required where to enforce the password combination requires of alphabets, numbers and symbols.

3.	**Proposed Process Flow**	**Item 1: Inability of the Internet Banking system to identify an account being activated using a different devices.** 1. To notify customer with the SMS alert or TAC to the customer's registered phone number for verification when her/his account is being activated using different device. a. Existing customer: Proposed KFH Online Login Steps:  Step 1 – Key in Username  Step 2 – Verify Security Phrase and key in Password  Step 3 – Customer will receive a TAC number to be keyed in to complete the signing (if customer login from a different device). Proposed Sample TAC: RM0.00 KFH: You are signed in KFH Online on a new device. TAC to complete the signing is xxxxxx. For queries, call 1300 888 534. b. New customer: For the new customer 1st time login is as per existing process. 2. For the device that is not activated or not being used for more than 90 days, it will be considered as a new device. The value is parameterized. 3. To disable concurrent or multiple login at one time, only single sign on is allowed. 4. TAC behavior/rules is as per existing.

		Item 2: Alphanumeric password to access Internet Banking account has yet to be enforced. Adoption of strong password for customers. To enforce the strong password with the combination of alphabets, number and symbol. a. Existing customer: i. System will force customer to change the password upon login to KFH Online. Proposed steps:  Step 1 – Key in username  Step 2 – Verify security phrase and key in password  Step 3 – System will prompt the Reset Password screen to enable customer to change the password. ii. The error message will be displayed if customer did not key in the combination of alphabets, number and symbol "Password is not a valid password. Password must be a mixture of alphabets, numbers and symbols". b. New customer: i. During the registration of KFH Online, the enforcement of strong password with the combination of alphabets, number and symbol is applied. ii. The error message will be displayed if customer did not key in the combination of alphabets, number and symbol "Password is not a valid password. Password must be a mixture of alphabets, numbers and symbols".
4.	**Charges**	Status-quo

5.	**Reports (new / enhancement) and samples**	New Corus report for item 1 – customer login from a different devices. Please refer as attached.
6.	**Audit Trails**	Yes
7.	**BVMC Changes / Enhancements**	N/A
8.	**Back-end processes / enhancements**	N/A
9.	**Timeline**	

New Corus report for item 1 – customer login from a new or different devices.



Sample Corus Report_Login New Device.xlsx - Excel

	A	B	C	D	E	F	G	H
1	Kuwait Finance House							
2	Report Name: Login New Device Report							
3	Generated Date: 01/06/2020 15:13:01							
4								
5	Date	RIM	Username	Customer Name	Mobile Phone No	Activity Type	Status	Reason
6	31/05/2020 00:02:34	111111	abc123	SITI NORIDAYU BINTI MOHAMAD SHAMSHUDIN	60172110000	Login from a new device	Successful	NIL
7	31/05/2020 00:03:37	222222	qwerty123	NORSHAFIRA AKMA BINTI AB MALEK	60172110000	Login from a new device	Unsuccessful	Wrong TAC keyed in for 3 attempts
8	31/05/2020 00:04:08	333333	asdf123	NUR EZZASAFFIQ BINTI ZULKIFLI	60172110000	Login from a new device	Successful	NIL
9								
10	Total Records	3						
11								

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

Telephone 60(3) 2698-8044 Jalan Dato' Onn
Facsimile 60(3) 2691-8850 50480 Kuala Lumpur
Web www.bnm.gov.my Malaysia

SULIT

Our Reference :

JPP/POL/4200/2/3/NMK/KK/RK/AS
15 April 2019

Ketua Pegawai Eksekutif
Licensed Banks
Licensed Islamic Banks
Prescribed Development Financial Institutions
Approved Electronic Money (E-Money) issuers (Mobile Payment Providers only)

Tuan/Puan,

Strengthening Measures to Mitigate Fraud through Phishing of SMS One Time Password (OTP)/ Transaction Authorisation Code (TAC)

The number of fraud cases related to the compromise of SMS OTP/TAC (SMS OTP/TAC fraud) for Internet banking and electronic money (e-money) transactions have increased since September 2018, involving several banking institutions and e-money issuers (collectively referred to as 'financial institutions'). SMS OTP/TAC which represented only 0.8% of total fraud[1] cases and 6.8% of total fraud[1] losses in March 2018, had increased to an average of 43.1% of total fraud[1] cases and 27.6% of total fraud[1] losses for the period from September 2018 to February 2019.

2. The modus operandi of SMS OTP/TAC fraud in recent cases involves the fraudster logging into the customer's Internet banking or e-money account via illegal means (e.g. stolen credentials through social engineering[2], brute force attack). The fraudster would subsequently contact the victim to obtain the SMS OTP/TAC to authorise the transfer of funds to mule accounts.

3. In order to address SMS OTP/TAC fraud more effectively, financial institutions need to intensify efforts to enhance customer awareness and ensure that the measures as listed in **Appendix I** are effectively implemented. Additionally, financial institutions are expected to implement the security measures as listed in **Appendix II.** If such security measures are not implemented**,** please provide alternative/compensating controls, if any, attested by Internal Audit as being similarly effective.

4. All financial institutions are required to submit the information in **Appendix II** to Bank Negara Malaysia no later than **15 May 2019**. Please do not

[1] Consist of Internet banking and mobile payments fraud.
[2] Customers were deceived into divulging their credentials (e.g. username, password/PIN and mobile number) to fraudsters via various channels (e.g. phishing website).

hesitate to contact Puan Kuldeep Kaur, Puan Ravinder Kaur or Encik Ahmad Shazwan at 03-2698 8044 ext. 8791, 8738 or 8136 respectively for any enquiries.

Sekian, harap maklum.

Yang benar,

(Tan Nyat Chuan)
Penolong Gabenor

Appendix I

Implementation of Measures to Enhance Customer Awareness to address SMS OTP/TAC Fraud

1. Financial institutions shall raise customer awareness on the safety measures that customers should undertake to counter SMS OTP/TAC fraud. Such steps include reminding customers of, but not limited to, the following:
   - The importance of SMS OTP/TAC as a key security feature while performing online transactions;
   - Not to share the SMS OTP/TAC and other login credentials (i.e. username, password and PIN) with any other party, even if the party requesting for such information claims to be from the financial institution, Bank Negara Malaysia or other authorities;
   - Common fraudsters' modus operandi. For example, the fraudsters may call and claim that his/her SMS OTP/TAC was wrongly sent to customer's mobile number and ask the customer to reveal the SMS OTP/TAC;
   - To create a strong password that uses a mixture of alphabets, numbers and symbols as well as to regularly change the password/PIN; and
   - To be wary of links sent via e-mail, instant messaging (e.g. WhatsApp, SMS) that may lead the customers to phishing websites.

2. In communicating the above reminders to customers, financial institutions shall ensure the following:
   - Multi-lingual communications are used to ensure a wide demographic reach. At a minimum, such communications must be provided in both Bahasa Malaysia (BM) and English; and
   - Messages are clear, simple and can be easily understood especially for customers in the more vulnerable segments e.g. senior citizens and B40 customers.

3. Reminders should be provided prominently through various channels, including web applications (e.g. push notifications within the financial institution's web-based interface), mobile applications (e.g. in-app notifications) and social media.

Appendix II

Implementation of Security Measures to address SMS OTP/TAC Fraud

		Current Measures (please describe)	**Timeline to implement** (if not yet implemented, where relevant)	**Alternative/ Compensating controls** (please describe)
1.	Ensure binding of mobile application to the customer's profile such as device ID and SIM card ID number/ account number			
2.	Verify with the customer when his/her account is being activated using a different[3] device. Such verification may be carried out via SMS to the customer's registered phone number			
3.	Deploy multi-factor authentication (MFA)[4] for the following transactions or actions:	*For each of the transaction/ action, please state the type of authentication method used.*		
	a) Internet banking/mobile banking/e-money account registration			
	b) Large value transactions	*To specify value*		
	c) Abnormal transaction behavior			

[3] Includes changes in mobile device, binding of additional device or login via a different device.

[4] Authentication methodologies shall be commensurate with the criticality of the functions by adopting a combination of two or more of the following three authentication factors: (i) something the user knows (e.g. password, PIN); (ii) something the user possesses (e.g. smart card, security device); and (iii) something the user is (e.g. biometric characteristics, such as a fingerprint or retinal pattern).

	d) Change in transaction limit (increase/reduce)			
	e) Change in password or PIN			
	f) Change in users' profile details (e.g. address, mobile number, etc.)			
	g) Change in response to challenge question			
	h) Adding of payment card for reload (for e-wallet mobile application)			
	i) Cash-out/withdrawal from e-money account			
	j) Others (please specify)			
4.	Customer's mobile number is masked at all times			
5.	Adoption of strong password for customers[5]			
6.	Conduct vulnerability assessment and penetration test on mobile application (e.g. brute force attack)			
7.	Implement effective fraud monitoring system/tools (e.g. adoption of behavioural analytics)			
8.	Customers receive instant notifications for any transactions made from their accounts			

[5] Strong password that cannot be easily predicted such as one that uses a mixture of alphabets, numbers and symbols.

Kuwait Finance House
بيت التمويل الكويتي

INTERNAL AUDIT REPORT

STRENGTHENING MEASURES TO MITIGATE FRAUD THROUGH PHISHING OF SMS ONE TIME PASSWORD (OTP) / TRANSACTION AUTHORIZATION CODE (TAC)

13 MAY 2019

Reference : IAD/BOIT-ITA/14-2019

RESTRICTED

LIST OF ABBREVIATIONS AND ACRONYMS

ACRONYMS	DETAILS
BNM	Bank Negara Malaysia
IB	Internet Banking
KFHMB	Kuwait Finance House (Malaysia) Berhad
MFA	Multi Factor Authentication
OTP	One-Time Password
SMS	Short Messaging System
TAC	Transaction Authentication Code

TABLE OF CONTENTS

Ref.	Contents	Page
1.0	BACKGROUND	1
2.0	SCOPE	1
3.0	CONCLUSION	1
4.0	VALIDATION ON IMPLEMENTATION OF MEASURES TO ENHANCE CUSTOMER AWARENESS TO ADDRESS SMS OTP / TAC FRAUD	2
5.0	VALIDATION ON IMPLEMENTATION OF SECURITY MEASURES TO ADDRESS SMS OTP / TAC FRAUD	3
6.0	APPENDICES	12

1.0 BACKGROUND

BNM, vide its letter dated 15 April 2019 to KFHMB, has raised its concern on increasing number of fraud cases related to compromised Short Messaging System One Time Password / Transaction Authorization Code **("SMS OTP / TAC")** for Internet Banking **("IB")** and electronic money. In order to address the fraud effectively, all Banks are required to intensify the efforts to enhance customer awareness and ensure the measures stipulated by BNM have been effectively implemented.

Internal Audit has been requested to attest the effectiveness of security measures and compensating controls implemented by KFHMB. The report shall be submitted to BNM within a month from the date of the letter, i.e. by 15 May 2019.

2.0 SCOPE

The scope of this review is to assess the effectiveness of the current and compensating controls in mitigating SMS OTP / TAC fraud risks, as listed in Appendix I and II of BNM letter dated 15 April 2019.

3.0 CONCLUSION

Assessment on the effectiveness of the controls to mitigate SMS OTP and TAC fraud risks performed between 6 May 2019 until 10 May 2019 consists of 11 main components and 16 sub-components of security measures. KFHMB has complied with 2 main components and 10 sub-components, while 2 main components and 2 sub-components security measures are not applicable as KFHMB is not offering services namely mobile application, e-wallet, e-money. The exceptions observed are as follows:-

3.0 SUMMARY OF AUDIT OBSERVATIONS

Ref	Observations	Action By	Target implementation date
Category I - Implementation of measures to enhance customer awareness to address SMS OTP / TAC fraud			
1.	Common fraudsters' modus operandi are not available in the social media i.e. Facebook and Instagram	Corporate Comm	CC to provide
2.	Reminders on phishing websites have yet to be communicated to customers through email and instant messaging e.g. WhatsApp, SMS	Corporate Comm	CC to provide
3.	Communications and reminders to customers using Bahasa Malaysia are currently not available	Corporate Comm	CC to provide
4.	Reminders not prominently displayed through social media	Corporate Comm	CC to provide
Category II - Implementation of security measures to address SMS OTP / TAC fraud			
5.	Inability of the Internet Banking system to identify an account being activated using a different customer's device	ITD	31.12.19 (to perform analysis)
6.	Multi-Factor Authentication **("MFA")** for abnormal transaction behavior not available. However, the compensating control to address the risk is effective	ITD	30.06.20
7.	Alphanumeric password to access IB account has yet to be enforced	ITD	30.06.20
8.	Errors in the fraud monitoring system in detecting abnormal behavior.	ITD	ITD to provide

4.0 VALIDATION ON IMPLEMENTATION OF MEASURES TO ENHANCE CUSTOMER AWARENESS TO ADDRESS SMS OTP / TAC FRAUD

No	Security Requirement	Compensating Controls	Validation by IAD
1.	Financial institutions shall raise customer awareness on the safety measure that customers should undertake to counter SMS OTP / TAC fraud. Such steps include reminding customers of, but not limited to, the following:- i. The importance of SMS OTP / TAC as a key security feature while performing online transactions; ii. Not to share the SMS OTP / TAC and other login credentials (i.e. username, password and PIN) with any other party, even if the party requesting for such information claims to be from the financial institution, Bank Negara or other authorities; iii. Common fraudsters' modus operandi. For example, the fraudsters may call and claim that his / her SMS OTP / TAC was wrongly sent to customer's mobile number and ask the customer to reveal the SMS OTP / TAC. iv. To create a strong password that uses a mixture of alphabets, numbers and symbols as well as to regularly change the password / PIN; v. To be wary of links sent via e-mail, instant messaging (e.g. WhatsApp, SMS) that may lead the customers to phishing websites.	Not applicable	Based on our observations at KFHMB's website, Facebook and Instagram accounts, we noted that: i. The SMS alert on importance of TAC was sent to all customers on 13 February 2019. **Refer Appendix I.** ii. Customer is alerted not to share SMS OTP / TAC and other login credentials in the security tips tab in KFHMB's corporate website as well as the online banking login page. iii. Fraudsters' modus operandi are available in the form of slides at the KFHMB's main website only. ***We recommend the same information to be shared in Facebook and Instagram.*** iv. Instruction on creating a strong password (mixture of alphabets numbers) as well as to change password frequently is available under the security tips tab in KFHMB's website. *v.* Reminders on phishing websites have yet to be communicated to customers through email and instant messaging. ***We recommend Corporate Communications to remind customers via social media on the need to be wary of phishing websites.***

No	Security Requirement	Compensating Controls	Validation by IAD
2.	In communicating the above reminders to customers, financial institutions shall ensure the following:- i. Multi-lingual communications are used to ensure a wide demographic reach. At a minimum, such communications must be provided in both Bahasa Malaysia (BM) and English; ii. Messages are clear, simple and can be easily understood especially for customers in the more vulnerable segments e.g. senior citizens and B40 customers.	Contact Centre staff are trained to speak in two (2) languages i.e. English and Bahasa Malaysia.	The communication for the above reminders to customer is only available in English language. ***We recommend Corporate Communications to extend the communications of the above reminders in Bahasa Malaysia.*** The messages are clear, simple and can be easily understood by customers in the more vulnerable segments.
3.	Reminders should be provided prominently through various channels, including web applications (e.g. push notifications within the financial institution's web-based interface), mobile applications (e.g. in-app notifications) and social media.	Not applicable	The reminders provided were found to be prominently displayed in the KFHMB's online banking login page website as well as in the security tips tab in KFHMB's corporate website. ***We recommend that reminders should also be provided through social media, which is currently not available.***

5.0 VALIDATION ON IMPLEMENTATION OF SECURITY MEASURES TO ADDRESS SMS OTP / TAC FRAUD

No		Current Measures (Described By Business Users / IT)	Timeline to Implement (if not yet implemented)	Alternative / Compensating Controls	Validation by IAD
1.	Ensure binding of mobile application to the customer's profile such as device ID and SIM card ID number / account number	KFHMB does not offer mobile application to customers.	KFHMB will ensure the requirement is addressed during the requirement stage for RPP QR Application and Mobile Token (Stronger 2FA). Target date: i. Quarter 1, 2020 (Mobile Token) ii. Quarter 2, 2020 (RPP QR)	Not available	KFHMB does not offer any mobile application to customers. **Conclusion** Not applicable.
2.	Verify with the customer when his / her account is being activated using a different[1] device. Such verification may be carried out via SMS to the customer's registered phone number.	The current Internet Banking system does not have the capability to identify when a customer's account is being activated using a different device.	Enhancement is required where an SMS alert will be sent when an IB account is being activated using a different device. Target date: Quarter 4, 2019 (to perform analysis)	Not available	The current Internet Banking system does not have the capability to alert the customer when account is being activated using a different device. **Conclusion** Security measures have not been complied.

[1] Includes changes in mobile device, binding of additional device or login via a different device.

No		Current Measures (Described By Business Users / IT)	Timeline to Implement (if not yet implemented)	Alternative / Compensating Controls	Validation by IAD
3.	Deploy multi-factor authentication **("MFA")**[2] for the following transactions or actions:				
a.	Internet banking / mobile banking / e-money account registration	Registration of IB requires MFA and the four (4) items are required:- i. Account number; ii. ATM card number; iii. ATM PIN; and iv. CAPTCHA[3] In addition, verification and activation by Contact Centre is required before customer logs in for the first time.	To strengthen the process by adding TAC as one of the steps in the registration process. Target date: Quarter 2, 2020	Not applicable	Registration of IB account requires the items listed below:- i. Account number; ii. ATM card number; iii. ATM PIN; and iv. CAPTCHA[4] **Refer Appendix II** The additional verification by Contact Centre is also required to activate a new IB account. **Conclusion** Security measures have been complied.

[2] Authentication methodologies shall be commensurate with the criticality of the functions by adopting a combination of two or more of the following three authentication factors: (i) something the user knows (e.g. password, PIN); (ii) something the user possesses (e.g. smart card, security device); and (iii) something the user is (biometric characteristics such as fingerprint or retinal pattern)

[3] Completely Automated Public Turing test to tell Computers and Humans Apart. A technique to distinguish between humans and computers; and mainly used as a security check to ensure only human users can pass through.

[4] Completely Automated Public Turing test to tell Computers and Humans Apart. A technique to distinguish between humans and computers; and mainly used as a security check to ensure only human users can pass through.

No		Current Measures (Described By Business Users / IT)	Timeline to Implement (if not yet implemented)	Alternative / Compensating Controls	Validation by IAD
b.	Large value transactions	KFHMB Internet Banking requires TAC for open transactions. However, open payments and transfer for RM10,000 and above have been disabled. Customers are required to register as favourite beneficiary to enable these transactions.	To strengthen the validation for large value transactions by adding stronger 2FA. Target date: Quarter 1, 2020 (Mobile Token)	Not available	Large value transactions are only permitted for "favourite beneficiary". Registration of favourite account will also require TAC, apart from the username and password which have been requested during login. **Conclusion** Security measures have been complied. **Refer Appendix III**
c.	Abnormal transaction behavior	KFHMB Internet Banking does not provide MFA for abnormal transaction behavior.	Target date: Quarter 2, 2020	Fraud detection system implemented in April 2019 is used to detect abnormal transaction behavior. Once a transaction hits the parameter configured in the fraud detection system, a security question will be prompted by IB system to authenticate the transaction.	A security question will be prompted by IB to authenticate abnormal transactions. **Conclusion** Security measures have not been complied. However, the compensating controls are effective. **Refer Appendix IV**

No		Current Measures (Described By Business Users / IT)	Timeline to Implement (if not yet implemented)	Alternative / Compensating Controls	Validation by IAD
d.	Change in transaction limit (increase / reduce)	TAC is required for changes in transaction limit.	Not applicable	Not applicable	TAC is required to change transaction limit, apart from the username and password which have been requested during login. **Conclusion** Security measures have been complied. **Refer Appendix V**
e.	Change in password or PIN	Forgot Password : i. Username; ii. Account number; iii. ATM card number; iv. ATM PIN number Change Password : 1. Old password; 2. New password; 3. Confirm new password; and 4. TAC number	Not applicable	Not applicable	Changing of password can be done either before a customer login to Internet Banking (via login page) or after a customer logged into IB (via Profile Maintenance). Both methods require MFA[5]. **Conclusion** Security measures have been complied. **Refer Appendix VI**
f.	Change in users' profile details (e.g. address, mobile number, etc.)	This function is not made available to customers in the Internet Banking.	Not applicable	Not applicable	Changing of users' profile details could only be done at Branches and Contact Centre. Internet Banking does not

[5] ATM card number is considered as something the user possesses. ATM PIN number is considered as something the user knows

No		Current Measures (Described By Business Users / IT)	Timeline to Implement (if not yet implemented)	Alternative / Compensating Controls	Validation by IAD
		Changing of users' profile details could only be performed at the Branches and validated by Contact Centre (for changing of mobile number).			provide the means for customers to change their profile details. **Conclusion** Security measures have been complied. However, we note that the mobile numbers maintained in ETHIX are not reflective of those maintained in Internet Banking database. Further review will be carried out on this exception.
g.	Change in response to challenge question	Forgot security answers : i. Username; ii. Account number; iii. ATM card number; iv. ATM PIN number Change security question and answers requires :- i. Username ; ii. Password; iii. TAC.	Not applicable	Not applicable	Changing of response to challenge questions could be done either before a customer login to Internet Banking (via login page) or after a customer logged into IB (via Profile Maintenance). Both methods require MFA[6]. **Refer Appendix VII** **Conclusion** Security measures have been complied.

[6] ATM card number is considered as something the user possesses. ATM PIN number is considered as something the user knows

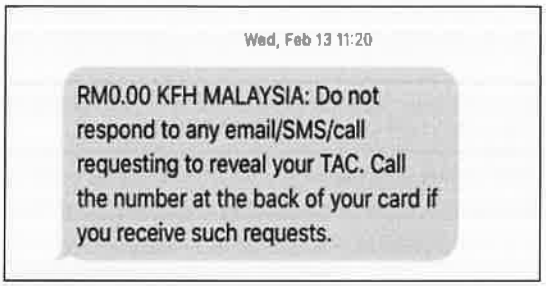
No		Current Measures (Described By Business Users / IT)	Timeline to Implement (if not yet implemented)	Alternative / Compensating Controls	Validation by IAD
h.	Adding of payment card for reload (for e-wallet mobile application)	KFHMB does not offer payment card for reload.	Not applicable	Not applicable	Not applicable
i.	Cash-out / withdrawal from e-money account	KFHMB does not offer e-money to customers.	Not applicable	Not applicable	Not applicable
4.	Customer's mobile number is masked at all times	Mobile number is masked if viewed via IB application.	Not applicable	Not applicable	**Conclusion** Mobile number is masked from customers' viewing. Security measures have been complied.
5.	Adoption of strong password for customers[7]	Password combination requires alphabets, number and symbols.	Target date: Quarter 2, 2020	Not available	Password combination requires alphabets, number and symbols. However, it is not enforced. **Conclusion** Security measures have not been complied.
6.	Conduct vulnerability assessment and penetration tests on mobile application (e.g. brute force attack)	KFHMB does not offer mobile application to customers.	Not applicable	Not applicable	Not applicable

[7] Strong password that cannot be easily predicted such as one that uses a mixture of alphabets, numbers and symbols

No		Current Measures (Described By Business Users / IT)	Timeline to Implement (if not yet implemented)	Alternative / Compensating Controls	Validation by IAD
7.	Implement effective fraud monitoring systems / tools (e.g. adoption of behavioural analytics)	Implemented in 26 April 2019	Not applicable	Not applicable	Three (3) detection modules implemented as follows:- i. Geolocation identification and detection of users; ii. Total daily transacted amount and frequency of transactions per day; iii. Maximum amount per transaction. However, the following gaps were observed:- i. The frequency of transactions does not capture accurate number of frequency; ii. The accumulated amount does not reflect the accurate number; iii. Normal transactions are captured in the report and triggered as abnormal transactions; iv. Missing transactions in the report; **Conclusion** Fraud monitoring system if not effective to detect abnormal behavior based on the samples reviewed.
8.	Customer receives instant notifications for any transactions made from their accounts	All monetary transactions will receive instant SMS notification	Not applicable	Not applicable	Customer will receive instant SMS notification after making a transaction via IB.

No		Current Measures (Described By Business Users / IT)	Timeline to Implement (if not yet implemented)	Alternative / Compensating Controls	Validation by IAD
					Conclusion Security measures have been complied.

Appendix I

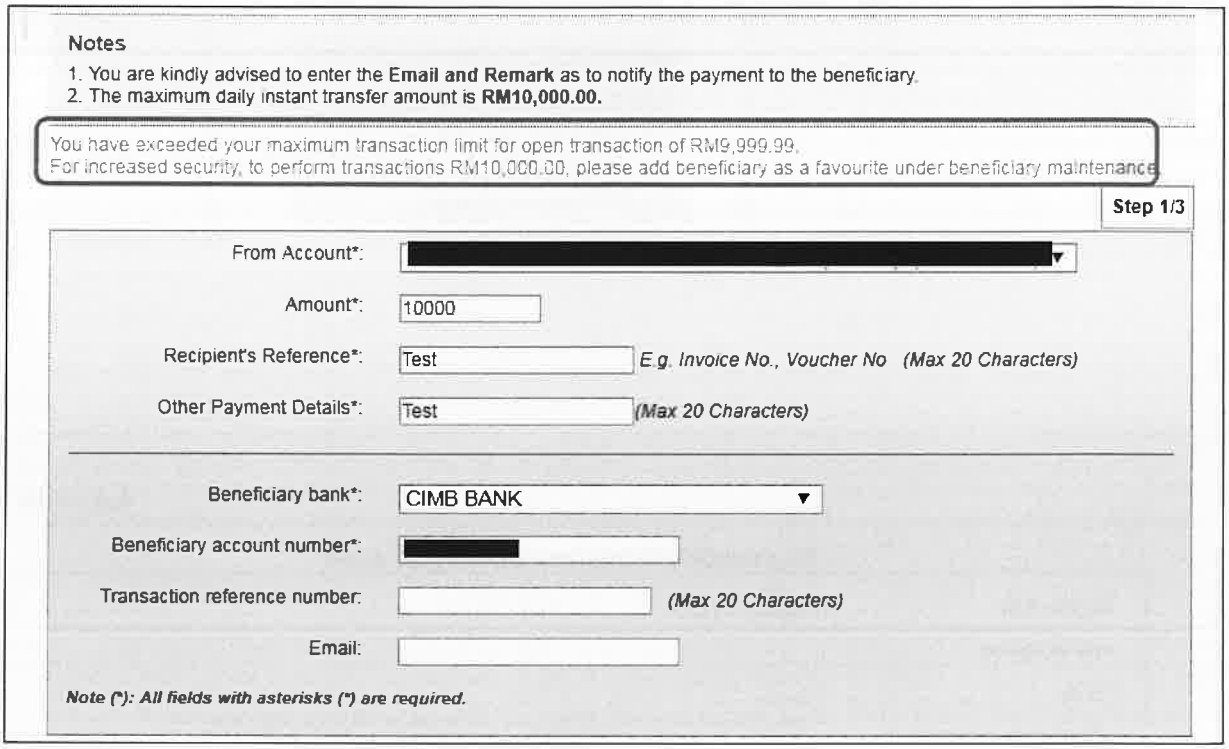


Appendix II

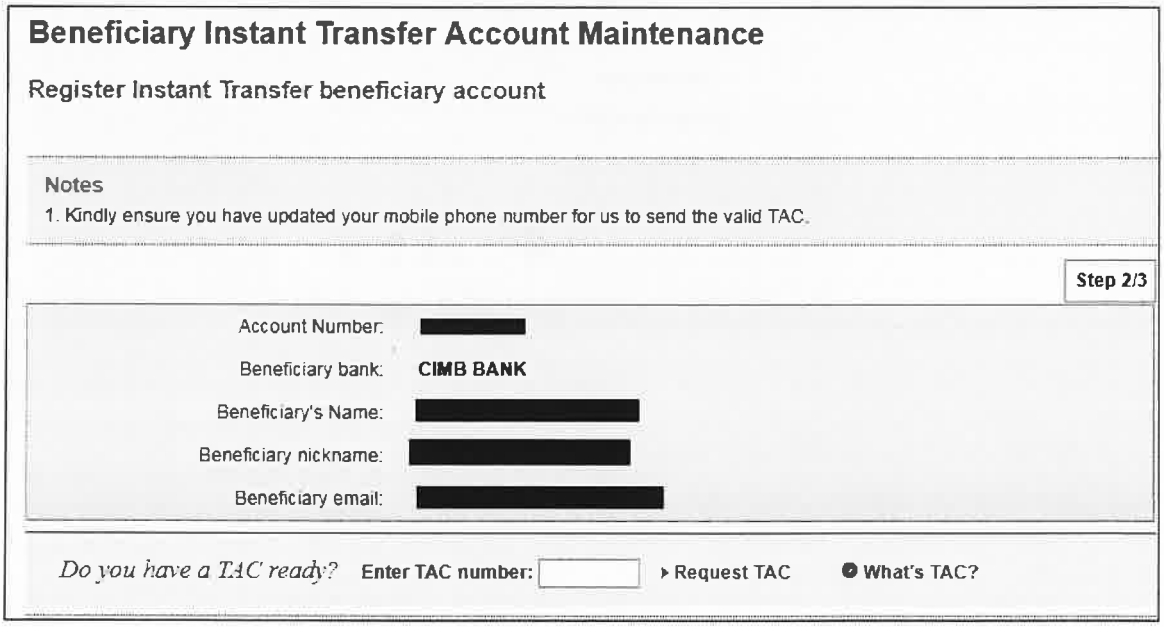
Registration of Internet Banking account

Appendix III

Posting to Open transaction of more than RM10,000

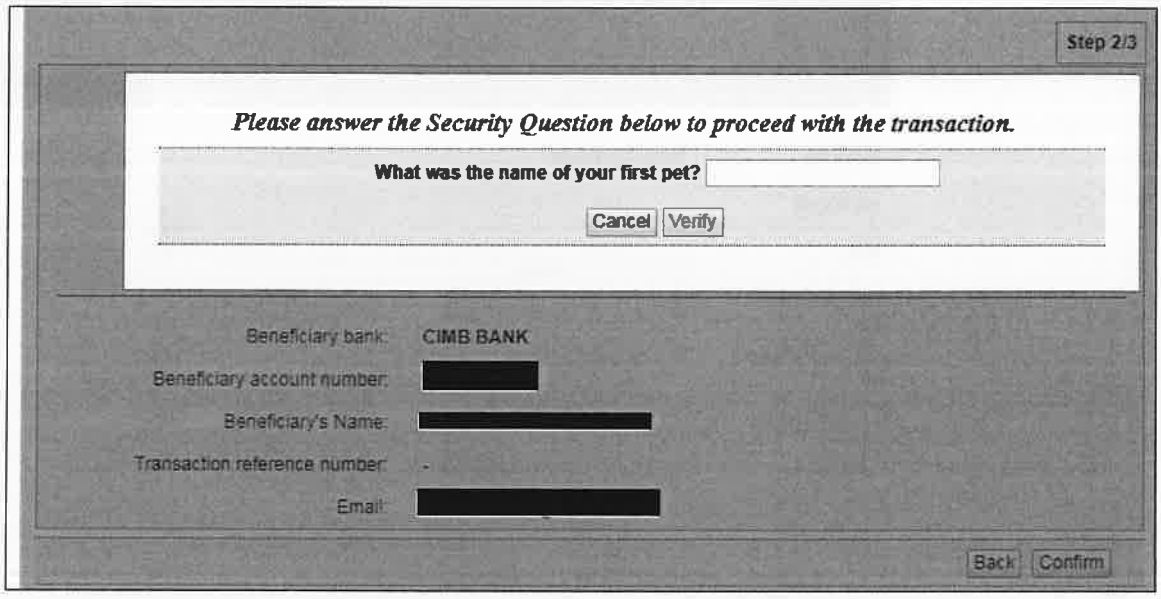


Registration of favourite beneficiary's account requires TAC



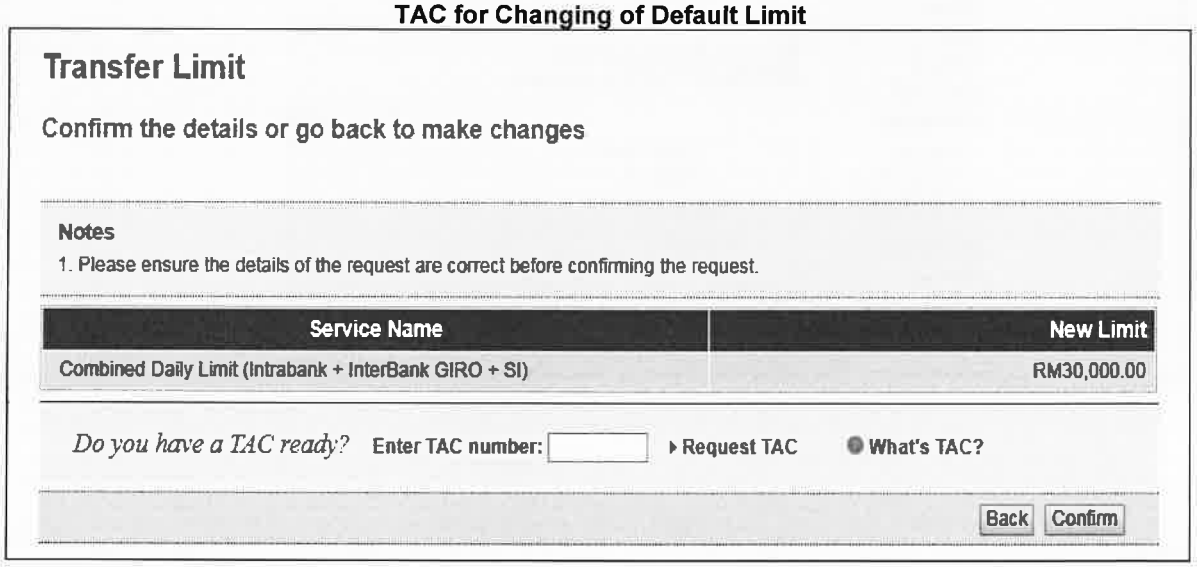
Appendix IV

Security question will be prompted to authenticate the transaction that has hit the abnormal parameter



Appendix V

TAC for Changing of Default Limit

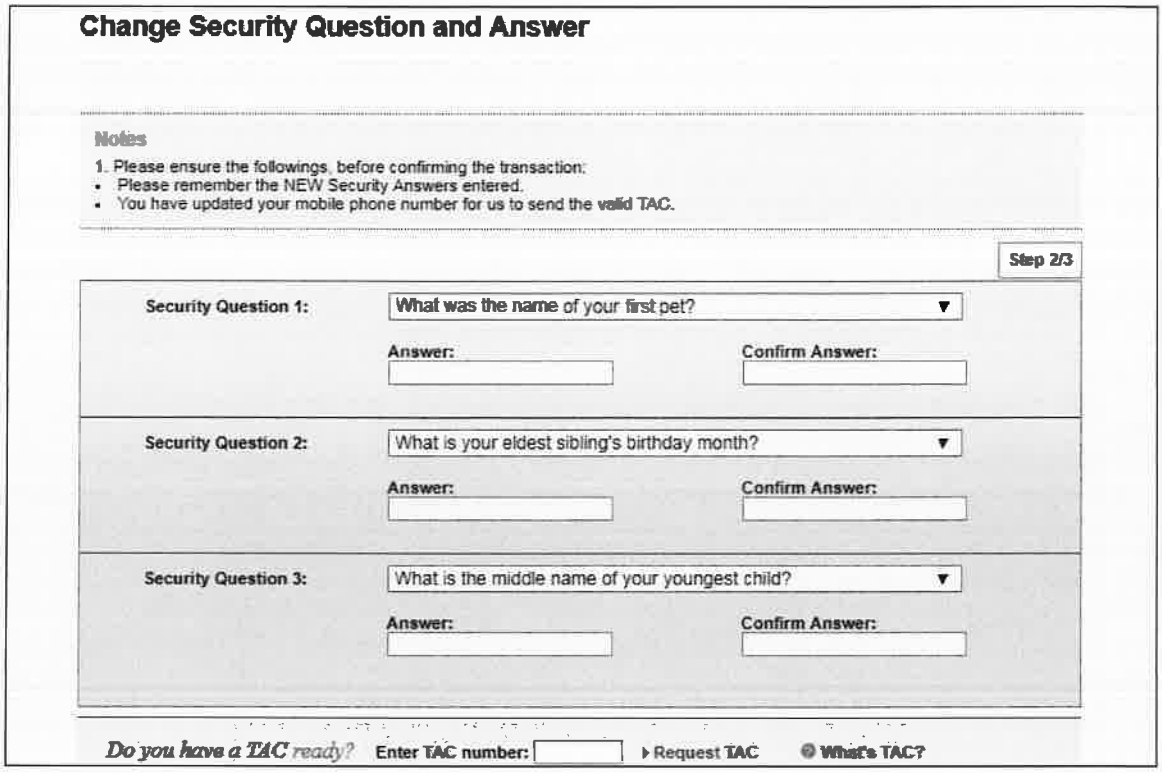


Appendix VI

Change of password via Internet Banking from login page

Change of password via Internet Banking

Appendix VII



Change Security Question and Answer

Notes

1. Please ensure the followings, before confirming the transaction:
   - Please remember the NEW Security Answers entered.
   - You have updated your mobile phone number for us to send the valid TAC.

Step 2/3

Security Question 1:	What was the name of your first pet?	
	Answer:	**Confirm Answer:**
Security Question 2:	What is your eldest sibling's birthday month?	
	Answer:	**Confirm Answer:**
Security Question 3:	What is the middle name of your youngest child?	
	Answer:	**Confirm Answer:**

Do you have a TAC ready? **Enter TAC number:** ▸ Request TAC ? What's TAC?