ACCOUNT MONITORNING PROCEDURE

When to refer this process?

On 25 February 2019, we will implement a new account monitoring system to provide additional security over our customers accounts and assist in reducing online fraud in real time.

The system learns legitimate trusted/returning customers' activities, historical fraud patterns and up-to-date fraud trends. This may prevent sophisticated fraudsters from completing the following activities:

- registering themselves for the Mobile App,
- logging in to Online Banking or Mobile App,
- making international transfers, and
- making external transfers.

Note: We are planning to implement a service which allows members to reset their Online Banking password by themselves via Online Banking. When this service is introduced, the account monitoring system will also monitor and assess the authenticity of the reset process.

This document explains the process to follow when a customer has been rejected from Online Banking or our Mobile App.

What kind of information will the system use to detect and reject potential fraud activities? (ONLY FOR INTERNAL INFORMATION)

The system will use a variety of information to determine potential risky behavior including:

- Device information
- Location information
- Information gathered by other companies who use this monitoring system (washed against global database)

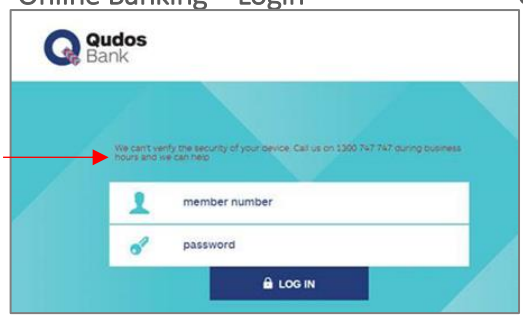
What will happen when the system detects a potential fraudulent activity?

The session will be automatically rejected, and an error message will be displayed saying:

"This action has failed as we can't verify the security of your device. You may wish to try again, however, if problems persist please call us during business hours for assistance on 1300 747 747 or +61-2-9582-3200 (if overseas)."

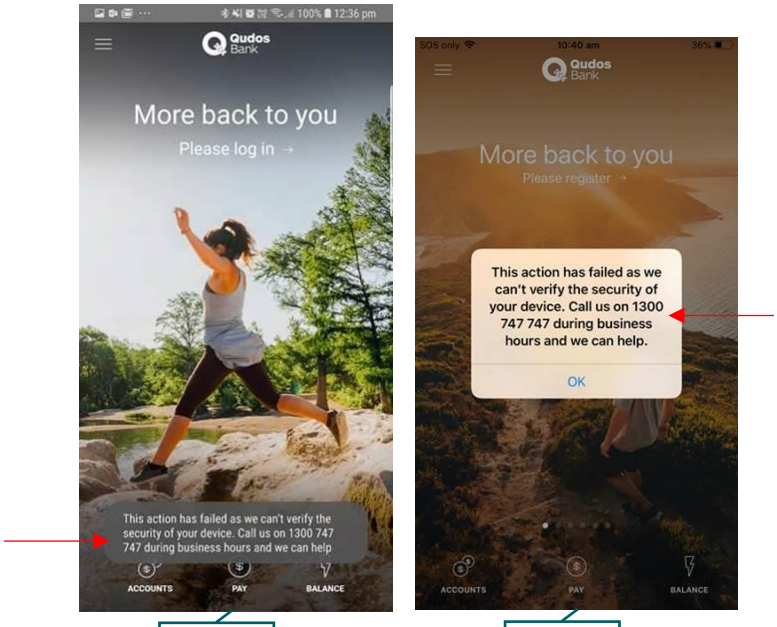
The messages shown in the below screenshots (→) will be replaced with the above message.

Online Banking – Login



Online Banking - Transfer

Mobile App - Registration, log-in and transfers



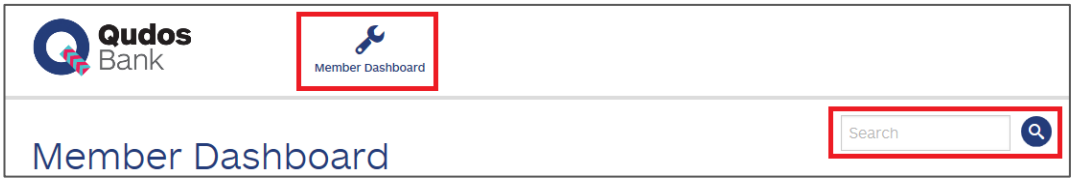
Note: The error message shown on Android devices will fade away in couple of seconds.

What to do if a customer calls / enquires about this message?

1. Complete the full ID verification process. Consult your supervisor if anything sounds suspicious.

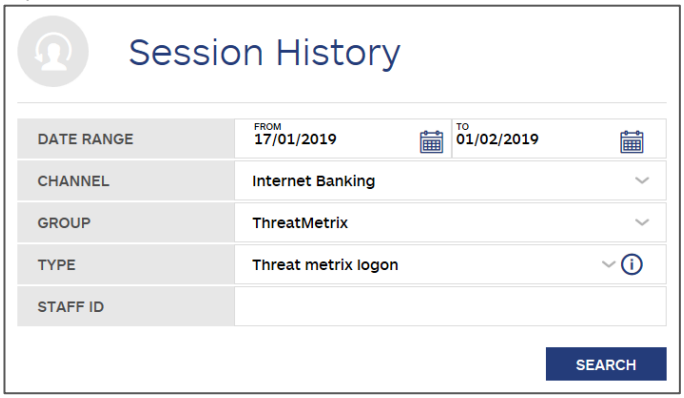
2. From the intranet, login to the IB Admin Console

3. Click the 'Member Dashboard' icon. Enter a RIM in the search box then click the search icon.



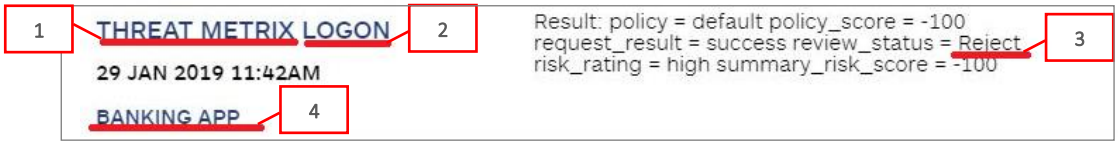
4. Click 'SESSION HISTORY.

Tip: The search results can be narrowed down by specifying the search information.



5. Confirm that the activity was rejected by the account monitoring system.

(continued)



	What does this indicate?
1	The account monitoring system intervention
2	The activity which the user attempted
3	The record showing that the activity was rejected by the monitoring system
4	If the activity was attempted by Mobile App, it shows 'BANKING APP'. If the activity was attempted by Online Banking, it shows blank. THREAT METRIX LOGON 29 JAN 2019 11:40AM Result: policy = default policy_score = -100 request_result = success review_status = Reject risk_rating = high summary_risk_score = -100

6. Ask **all** the following questions.

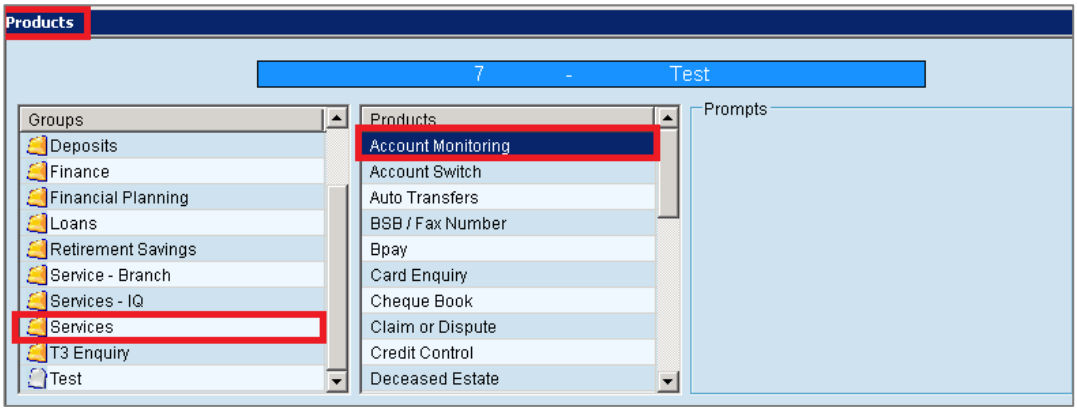
Question 1: **Are you using the device which you normally use?**
If no, ask the user to try it again with a safer device (e.g. the device the user normally uses or PC at branch) while on the phone/at the branch.
Question 2: **Have you recently been contacted by someone that has requested access to your computer?** **Have you been instructed by this person to make a transfer?**
If the answer to any of these questions is "Yes", it needs to be referred to the fraud team (fraudwarnings@qudosbank.com.au) by email.
Question 3: **Do you actually know the payee who you are trying to make a payment?**
If the answer to this question is "No", say to the customer: "Our account monitoring system has identified this as an unusual transaction that requires verification. If you still want to proceed, you may not be able to recover the funds if you later dispute the transaction. Do you still want to proceed"?

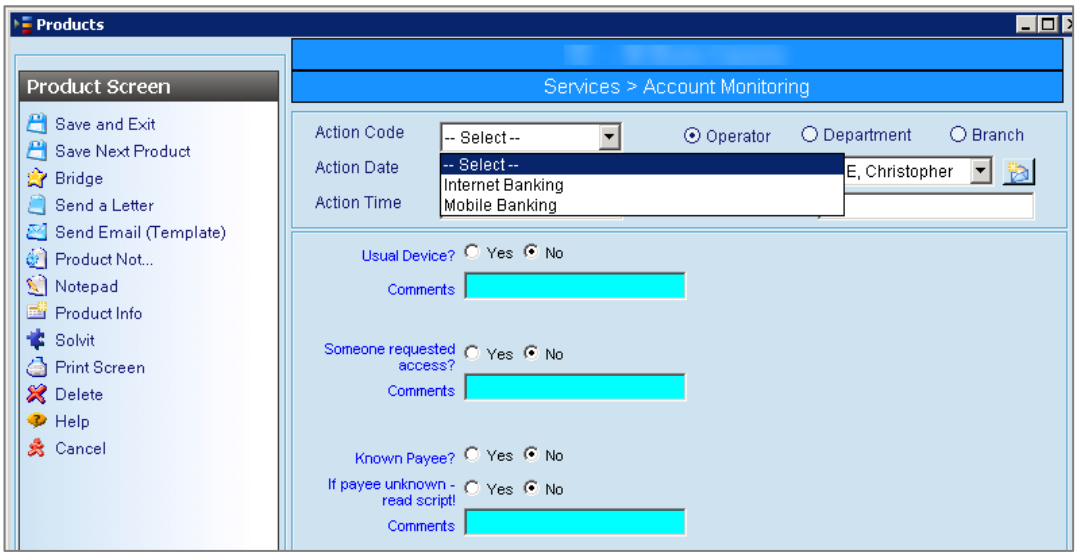
(continued)

7. If the system still rejects the activity, advise the customer that you need to refer to other teams to have a look at this further. Email fraudwarnings@qudosbank.com.au including the answers to the questions in Step 6 and the user's contact information.

   Note: If the fraud team needs to speak to the customer for further information, they will contact them directly. Otherwise the fraud team will make necessary adjustments by 10am the next business day which allows the customer to do the activity again. If you would like to be notified when the fraud team completes the adjustments (so that you can contact the customer to ask them to try it again etc.), put your request in the email.

8. Leave a detailed Prosper note **(Products → Services → Account Monitoring → Action Code -Internet Banking/Mobile Banking)** including the answer to the questions in Step 6.





FAQ

Customer FAQ

Q1. "What account monitoring system does Qudos Bank use? How does it work?"

A1. "We have various fraud monitoring initiatives in place to protect your accounts. The various solutions we use assist with fraud prevention, authentication and threat detection across our core banking system. It helps us to validate returning customers (and detects potential cybercriminal activity.

ORION is our card fraud monitoring partner and provides our customers with 24/7 card monitoring services ensuring the security of your card is maintained at all times.

The Orion card fraud management service monitors, identifies and takes action on suspect card transactions. This is why it's important you advise us when you're travelling overseas.

In addition to our fraud monitoring initiatives we also recommend that you take personal precautions to keep passwords safe and secure, only use trusted sites and never allow third parties to access your devices."

Q2. (From the user whose activity was blocked) "Why was my registration/log-in/ transfer rejected?"

A2. "There could be a number of reasons why your transaction was rejected, could I ask you a couple of questions so we can investigate further?"

Q3. (From the user whose activity was blocked) "What should I do to avoid that in the future?"

A3. The response could be dependent on the issue encountered.
Ensuring the customer is using a trusted device that they normally use to log in to Online Banking / Mobile App could assist.

Contact for help

Contact your immediate supervisor or the Fraud team for help.

Version Control

Date	Reviewed by	Purpose / Change
13/02/2019	Antar C Cameron S Devika S Dimitrios K Jill K Loren I Michelle N Nimin J Vikas K	V1.1 - Creation of the document V1.2 – Revision of step 8: Prosper screenshot