Central Bank of Oman

البنك المركزي العماني

RECEIVED
11 JUN 2019
BankDhofar - HO
CEO'S Office

BDD/CBS/CB/2019/3287

10 June 2019

URGENT

To: All Licensed Banks
Operating in the Sultanate of Oman

After compliments,

Sub: OmanNet Payment Gateway Security Regulations & Guidelines

1. The mobile and payments ecosystem is complex and dynamic. While security capabilities are evolving, attackers continue to explore new avenues, including through mobile devices, to commit malicious activities such as sensitive data exfiltration or fraud.

2. In order to establish a level of confidence in the security of mobile payment applications and align security controls, Central Bank of Oman wishes to publish minimum-security requirements for merchants using e-commerce acquiring service in Oman.

3. Considering the fact that acquirer banks are responsible for certifying and onboarding of merchants to use the Payment Gateway service, it is the responsibility of the acquirer bank to ensure that every merchant is compliant with the security requirements mandated as under:-

   i) Merchant acquirer banks are required to obtain "self-assessment questionnaire", (as per the annexure) completed by all online merchants operating in Oman, duly signed by the authorized representative of the merchant establishment. On receipt of the same from the merchants, the "Merchant Acquirer Bank" is required to submit the said completed self-assessment questionnaire to, the Manager, Information

ص.ب : ١١٦١، روي، الرمز البريدي: ١١٢، سلطنة عمان، هاتف : ٢٤٧٧٧٧٧٧ ، فاكس : ٢٤٧٧٧٧٣٣
P.O. Box 1161 Ruwi, Postal Code 112, Sultanate of Oman - Tel.: 24777777- Fax: 24777733
http://www.cbo.gov.om

Security Management Department of the Central Bank **on or before September 1, 2019**.

ii) Acquirer Banks are also mandated to make completion of this Security self-assessment questionnaire a pre-requisite for any new merchant on-boarded for processing e-commerce payment in the country.

iii) Acquirer Banks should also obtain such completed self - assessment questionnaire from all the online merchants on annual basis and retain the same for the purpose of verification by CBO examiners and auditors.

4. In this regard, for any further information or clarification, licensed banks may contact the Information Security Management Department email: information.security@cbo.gov.om.

5. Banks are advised to be guided accordingly.

Best regards,

Malik Abdullah Al Mahrooqi
Vice President
Banking Oversight

Encl.: as above

Annexure to Circular letter no. BDD/CBS/CB/2019/3287 dated June 2019

Payment Gateway Security Controls
Merchant Self-Assessment

Merchant Name	
Merchant Application	
Commercial Bank Name	
Date	

Merchants are required to comply with the Security Controls and fill in a self-assessment for EACH merchant application. Forms are to be duly submitted to the merchant's acquiring bank.

Central Bank of Oman strongly recommends merchant to:

- Utilize the OWASP Mobile Application Security Verification Standard (MASVS-L1) as a baseline for mobile application security.
- Strive to be compliant to the Payment Card Industry Data Security Standard (PCI DSS) if directly capturing card data.

Note: Liability of any loss due to insufficient controls on the merchant systems will be solely the merchant's responsibility.

Annexure to Circular letter no. BDD/CBS/CB/2019/3287 dated June 2019

	Functional Controls	Compliant	Not Compliant	Comments
M.1	The request page from where the merchant sends the initial request to Payment Gateway is securely stored at merchant environment and is not available at internet	☒	☐	
M.2	The resource file, alias name, tranportal ID, tranportal password are securely stored in merchant environment and is not accessible outside via internet or other means	☐	☐	
M.3	Ensure that Session IDs are randomly generated on the server side.	☐	☐	
M.4	System must be able to identify and block duplicate requests.	☐	☐	
M.5	Ensure that the system only accepts Response messages directly from Payment Gateway by validating the Payment Gateway IP/domain.	☐	☐	
M.6	The Merchant backend server must verify the user's session ID and transaction amount from the Payment Gateway RESPONSE MESSAGE to verify that the amount paid is equivalent to requested payment amount. The transaction amount in the Payment Gateway Response message must be depicted in the Merchant application database.	☐	☐	
M.7	Securely store the transaction response in your secured database before redirecting to the customer on the result page	☐	☐	
M.8	Communicate transaction response to the card holder only by querying/fetching the response from your secured database	☐	☐	

Annexure to Circular letter no. BDD/CBS/CB/2019/3287 dated June 2019

	Technical Controls	Compliant	Not Compliant	Comments
M.9	System must employ sufficient logging and log both Payment Gateway requests and responses.	☐	☐	
M.10	DO NOT use bank provided demo/sample web pages/codes for production applications	☐	☐	
M.11	The use of out-of-support/end-of-life operating systems software in merchant backend is restricted. Ensure that merchant systems are patched and kept up to date.	☐	☐	
M.12	Ensure that a mechanism for enforcing updates of the mobile app exists and the software is patched and up to date.	☐	☐	
M.13	Ensure that the application detects, and responds to, the presence of a rooted or jailbroken device either by alerting the user or terminating the app.	☐	☐	
M.14	Ensure that the application prevents debugging and/or detects, and responds to, a debugger being attached.	☐	☐	
M.15	Ensure that the application detects, and responds to, tampering with executable files and critical data within its own sandbox.	☐	☐	
M.16	Ensure that the application detects, and responds to, the presence of widely used reverse engineering tools and frameworks on the device.	☐	☐	
M.17	Ensure that the application detects, and responds to, being run in an emulator, tampering to the code and data in its own memory space.	☐	☐	
M.18	Ensure that the application implements a 'device binding' functionality using a device fingerprint derived from multiple properties unique to the device.	☐	☐	

Annexure to Circular letter no. BDD/CBS/CB/2019/3287 dated June 2019

	Procedural Controls	Compliant	Not Compliant	Comments
M.19	Implemented a daily reconciliation process to reconcile transaction details as per your system/database against transaction details as per Payment Gateway/settlement report.	☐	☐	
M.20	Implement a reporting process to report any identified gaps	☐	☐	
M.21	Merchants to use automated transaction enquiry message for OmanNet hosted payment page transactions	☐	☐	