Company Policy and PCI-DSS Audit Report

Date: June 6th, 2025

Auditor: J. Fluker

Table of Contents

Executive Summary

The following is an assessment of Globomantics to ensure that it is compliant with its company policy as well as the Payment Card Industry Data Security Standard (PCI DSS).

After conducting interviews with the Active Directory Administrator, Senior System Engineer, Helpdesk Analyst, and Head of Learning and Development, I concluded that Globomantics is compliant with its information security policies 14.1 through 14.4. It is also compliant with PCI DSS requirements 8.3.1 through 8.3.4 and requirement 8.3.7.

Globomantics is not compliant with requirement 8.3.5, 8.3.6, and 8.3.8.

*Requirement 8.3.9 is not applicable due to Globomantics' use of multifactor authentication.

Key findings:

- The process for selecting a unique password is inconsistent between helpdesk analysts
- Frequent re-use of temporary passwords (such as Password1)
- Active directory is configured to require a minimum length of 8 characters
- Inefficient instructions regarding the reuse of internal passwords

To address these issues and meet compliance, Globomantics should: Restrict the procedure for selecting a unique password to one effective method, ban the re-use of temporary passwords, increase the minimum password length from 8 to 12, and update the Acceptable User Policy and training material to instruct employees to change passwords/passphrases if they have any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.

Objective and Scope

Evaluating whether Globomantics is in compliance with its Information Security Policy and the Payment Card Industry Data Security Standard (PCI DSS) is the objective of this assessment. Polices evaluated focused on authentication. I assessed the following requirements:

- **Information Security Policy:** Requirements 14.1 through 14.4

- **Payment Card Industry Data Security Standard (PCI DSS):** Requirements 8.3.1 through 8.3.9.

The scope of this assessment included verifying the effectiveness and identifying vulnerabilities of Globomantics' access controls (passwords, multi-factor authentication, smart card, authorization, user account management), and its security awareness.

Methodology

To assess whether Globomantics is in compliance, I interviewed the following Globomantics team members: Tom Robertson: Active Directory Administrator, Charlotte Khan: Senior Systems Engineer, Aaron Lee: Helpdesk Analyst, and Frank Stone: Head of Learning and Development.

I also reviewed documentation and tested policies using the Payment Card Industry Data Security Standard (PCI DSS) Version 4.0, requirement 8.3.

These requirements ensure that strong authentication for users and administrators is established and managed.

I tested requirements 8.3.1 through 8.3.9 for the assessment.

Globomantics Information Security Policy

Section 14: Authentication

- **14.1** Multifactor authentication by password and Globomantics smart card is required for access to all systems.

- **14.2** Passwords must be:
    - 14.2.1 At least eight characters
    - 14.2.2 Complex (as defined by Active Directory)
    - 14.2.3 Changed every 90 days

- **14.3** Accounts must:
    - 14.3.1 Be locked after 3 incorrect password attempts and
    - 14.3.2 Remain locked until they are manually reset by the Globomantics helpdesk

- **14.4** Employees must quote badge ID and secret word to have their password reset

Payment Card Industry Data Security Standard Version 4.0

Requirement 8.3: Strong authentication for users and administrators is established and managed.

Requirements 8.3.1 through 8.3.9

- **8.3.1** All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:
  - Something you know, such as a password or passphrase.
  - Something you have, such as a token device or smart card.
  - Something you are, such as a biometric element

- **8.3.2** Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components.

- **8.3.3** User identity is verified before modifying any authentication factor.

- **8.3.4** Invalid authentication attempts are limited by:
  - Locking out the user ID after not more than 10 attempts.
  - Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed.

- **8.3.5** If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:
  - Set to a unique value for first-time use and upon reset.
  - Forced to be changed immediately after the first use.

- **8.3.6** If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity:
  - A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters)
  - Contain both numeric and alphabetic characters.

- **8.3.7** Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used.

- **8.3.8** Authentication policies and procedures are documented and communicated to all users including:
  - Guidance on selecting strong authentication factors.
  - Guidance for how users should protect their authentication factors.
  - Instructions not to reuse previously used passwords/passphrases.
  - Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident.

- **8.3.9** If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either:
    - Passwords/passphrases are changed at least once every 90 days, or
    - The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly.

Findings

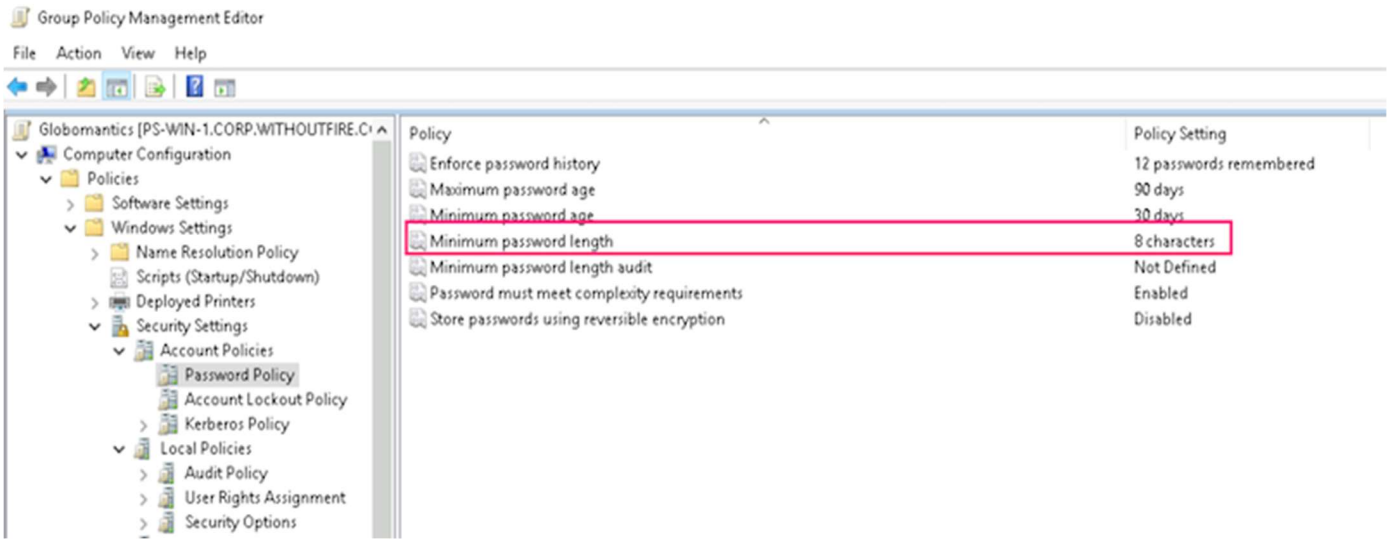
Globomantics is compliant with information security policies 14.1 through 14.4. It is also complaint with the Payment Card Industry Security Standard (PCI DSS) requirements 8.3.1 through 8.3.4 and requirement 8.3.7. However, Globomantics is not compliant with requirement 8.3.5, 8.3.6, and 8.3.8.

Requirement 8.3.5

Although new user accounts are set up with a unique password and forced to be changed at first use, when passwords are reset by the helpdesk, the process for selecting a unique password is inconsistent between helpdesk analysts. The frequent re-use of temporary passwords (such as Password1) could undermine the company's goals and leave it vulnerable to an attacker using brute force software -- a method that could crack passwords in minutes.

Requirement 8.3.6

Payment Card Industry Security Standard requires a minimum password length of ***12*** characters. However, Globomantics policy 14.2 only requires a minimum password length of ***8*** characters. This is reflected in its active directory. **(See image below for an example)**



Requirement 8.3.8

Globomantics' Acceptable User Policy (AUP) as well as the training course it provides does not advise its employees to not reuse passwords, nor does it provide any instructions for employees to change passwords/passphrases if there is any suspicious activity or knowledge that the password/passphrases have been compromised, and how to report an incident.

***Requirement 8.3.9**

I deemed requirement 8.3.9 **Not Applicable** due to Globomantics' use of multifactor authentication.

Other Observations

After reading the PCI DSS documentation, I concluded that the PCI DSS assessor will need to see the encrypted password store and a packet capture to validate that passwords are encrypted in storage and in transit.

Charlotte Khan (Senior System Engineer) informed me that this would require a ticket to be raised in the engineering system which would need to be approved by the CISO. We need to make sure we do this before the external assessment is scheduled.

Some of Globomantics' password policies such as changing every 90 days and locking out after three incorrect attempts were put in place before they introduced smart cards, when a password was the only authentication factor in use.

Best practice from NIST and the UK National Cyber Security Centre is not to force such frequent password changes.

PCI DSS does not require forced changes if the password is not the only authentication factor in use. Additionally, the helpdesk reported that many of their calls were for password resets. In the future, we should ask the risk team to re-evaluate these Globomantics policies.

When a user's initial account is set up, their temporary password is set to a combination of the number printed on their smartcard and their name. Technically this is single factor authentication as the smartcard (which also has the colleague's name printed on it) is the only single factor required to gain access to the systems until the user first logs in and changes the password. This practice should be reviewed by risk.

Overview of Globomantics Information Security Policy Compliancy

(Section 14: Authentication)

Policy ID	Status
Policy 14.1	Compliant
(Policy 14.2) 14.2.1	Compliant
Policy 14.2.2	Compliant
Policy 14.2.3	Compliant
(Policy 14.3) 14.3.1	Compliant
Policy 14.3.2	Compliant
Policy 14.4	Compliant

Overview of Globomantics PCI-DSS Compliancy

(Requirements 8.3.1-8.3.9)

Requirement ID	Status
Requirement 8.3.1	Compliant
Requirement 8.3.2	Compliant
Requirement 8.3.3	Compliant
Requirement 8.3.4	Compliant
Requirement 8.3.4 (part 2)	Compliant
Requirement 8.3.5	Compliant
Requirement 8.3.5 (part 2)	Not Compliant
Requirement 8.3.5 (part 3)	Compliant
Requirement 8.3.6	Not Compliant
Requirement 8.3.6 (part 2)	Compliant
Requirement 8.3.7	Compliant
Requirement 8.3.8	Not Compliant
Requirement 8.3.9	Not Applicable

Recommendations

To address areas of non-compliance and to improve security, Globomantics should:

1. Restrict the procedure for selecting a unique password to one effective method to reduce severity of brute force attacks.

2. Ban the re-use of temporary passwords to protect against certain cyber attacks such as phishing and to avoid multiple security breaches.

3. Increase the minimum password length from 8 to 12, not just to meet compliance, but to defend against dictionary attacks. (Method utilized by hackers to systematically try common words and phrases from a dictionary of potential passwords.)

4. Update the Acceptable User Policy and training material to instruct employees to change passwords/passphrases if they notice any suspicious activity or know of any password/passphrases that have been compromised.

5. Employees should also have clear instructions/documentation on how to report suspicious activity, ensuring everyone remains informed should an incident occur.

If you have any questions, I'm available at the following address:jkinfluker@gmail.com

Thank you,

J. Fluker

GRC Analyst