PCI DSS 6.4.3 and 11.6.1 FAQ

The intent of the new requirements in sections 6.4.3 and 11.6.1 of PCI DSS 4.0 is to enhance the security of online payments and ensure proactive security management. We recommend referring to guidance from Foregenix, our Qualified Security Assessor (QSA), in their blog post [here], as well as the official PCI Security Standards Council (PCI SSC) website [here] for additional FAQs and compliance details.

Key Takeaways:

- Each party involved in online payments plays a role in ensuring data security.
- The requirements apply to both mobile applications and websites.
- There is no one-size-fits-all approach to compliance; however, inaction is not an option.

NMI's Compliance Approach

To address these requirements, NMI has implemented the following measures:

- Content Security Policy (CSP) implementation
- Comprehensive script inventory with documented justifications
- Integration of scripts into our File Integrity Monitoring (FIM) tool
- Ongoing vulnerability scans
- Regular penetration (PEN) testing
- Dedicated web application security testing

Secure NMI URLs

To ensure security and compliance, NMI only provides the following secure URLs for integration:

API Integration URLs:

- https://secure.networkmerchants.com/api/transact.php
- https://secure.networkmerchants.com/api/v2/three-step
- https://secure.usaepay.com/api/v2/

JavaScript URLs:

- https://secure.networkmerchants.com/js/v1/Gateway.js
- https://secure.networkmerchants.com/token/Collect.js

QuickClick (Shopping Cart Integration):

- https://secure.networkmerchants.com/cart/cart.php

WebMIS Virtual Terminal:

- https://webmis.creditcall.com/mobile/login.php
- https://webmis.creditcall.com/login.php

Hosted Payment Page:

- https://live.ekashu.com

3D Secure Integration:

- https://3ds2s.cardeasexml.com:9603

Query API (Reporting):

- https://secure.networkmerchants.com/api/query.php

Additionally, integrations are secured according to the specifications provided by NMI. NMI utilizes DigiCert and GoDaddy for digital certificate issuance.

Note: Webhook integrations are not listed here, as they are defined by the integrator.

Security Measures and Recommendations

- **Content Security Policy (CSP):** Helps ensure that only authorized scripts are loaded, supporting compliance with PCI DSS Requirement 6.4.3.
- **Script Inventory and Justification:** Reducing the number of scripts minimizes the attack surface, while maintaining a documented inventory enhances security control.
- **Webpage Integrity Tools:** These tools provide real-time alerts for unauthorized script changes and help prevent malicious activity.
- **Requirement 11.6.1 in PCI DSS v4.0.1:** The update clarifies that only changes affecting the security of cardholder data require monitoring under file integrity monitoring (FIM) requirements.
- **Environment Maintenance:** Keeping systems updated with the latest patches, securing plugins and add-ons, and deploying antivirus/malware protection are critical for compliance.
- **Thorough Testing:** All changes should be fully tested in a non-production environment before being deployed to production.

Solution-Specific Considerations

eKashu

- Merchants using the eKashu hosted payment page, as implemented per NMI instructions, should remain eligible for SAQ A without additional controls under 6.4.3. NMI fully manages eKashu's security and compliance.

QuickClick Omni

- The 'Allow Merchant To Use Inline JavaScript' feature permits custom scripts. However, NMI does not validate merchant-defined JavaScript. Merchants are responsible for ensuring script security each time an update is made.

USAePay Payment Forms (V1 & V2)

- If external scripts are added without a CSP policy, they are saved as unparsed templates.
- Similar to QuickClick, NMI cannot validate custom scripts, and merchants must self-validate and revalidate upon updates.

Important: Users of QuickClick Omni and USAePay Payment Forms with custom scripts are **fully responsible** for security validation. NMI does not provide script validation or assume responsibility for security risks.

Frequently Asked Questions (FAQs)

Q: Can we use SRI (Subresource Integrity) for script validation?

- While SRI (Subresource Integrity) can be an additional security measure, NMI has focused on CSP and nonce-based security as primary controls. Merchants implementing SRI must ensure CORS (Cross-Origin Resource Sharing) headers allow script validation.

Q: Can USAePay include a Permissive CORS header?

- While we recognize the request for Access-Control-Allow-Origin: *, NMI strongly recommends against caching or locally hosting scripts. Scripts should be loaded from NMI's designated URLs to ensure security and compliance.

Final Notes

Since NMI has limited visibility into your cardholder data environment, we can provide only general guidance. We strongly recommend consulting a PCI Security Standards Council-certified Qualified Security Assessor (QSA) for detailed compliance requirements under PCI DSS 4.0 and v4.0.1 updates.

For further information, please refer to the PCI Security Standards Council website or contact your QSA. If you have additional questions regarding NMI's security implementations, please reach out to your account representative.