

Logo

Description automatically generated

**State of New Mexico**

**PCI Website Audit Report – Wave {{WAVE\_NUMBER}}**

**{{CLIENT\_NAME\_FULL}}**

**Date of site audit: {{DATE\_OF\_SITE\_AUDIT}}**

**Date of report transmitted to client: {{DATE\_OF\_REPORT\_TO\_CLIENT}}**

**Table of Contents**

[Overview 3](#_Toc119145257)

[Purpose 3](#_Toc119145258)

[Action May Be Required 3](#_Toc119145259)

[Scope – Number of URLs (as provided by the Agency) 3](#_Toc119145260)

[Methodology 4](#_Toc119145261)

[Audit Summary 5](#_Toc119145262)

[Detailed Report 6](#_Toc119145263)

## Overview

The State of New Mexico Department of Finance and Administration (DFA) contracted with Securin Inc. (Securin), an affiliate of Ivanti, to monitor all payment-card-accepting Agencies’ externally facing websites for the presence of card payment purchase functionality. This audit identifies the URLs with payment options by manually browsing the list of URLs shared by the Agencies. This report summarizes the shared URLs leading to payment pages, and whether those payment URLs are PCI-compliant or not.

Monitoring includes Agencies which have reported through audits that the web channel is being used for consumer and/or business payments. SECURIN will perform the following:

* Visiting all in-scope Agencies’ websites based on the list provided by the Agencies
* Identify if Agencies are accepting payment cards
* Cataloging proof of payment screen presence via screen grab (but without making a purchase)

During the audit, links which were not accessible and/or which showed errors while accessing, and those which require credentials, were not accessed for compliance. In these cases, further action is required from the Agency. Please refer to the detailed section of the report for more information.

## Purpose

The purpose of the audit is to identify the payment accepting Agencies' URLs and whether those payment URLs are PCI-compliant (or not). If any Agencies’ sites are found to be non-compliant the same will be informed officially to DFA.

## Action May Be Required

See detail beginning on “Audit Summary” page.

## Scope – Number of URLs (as provided by the Agency)

|  |  |
| --- | --- |
| **Agency** | **Number of URLs** |
| {{AGENCY\_ABBREVIATION}} | {{NUMBER\_OF\_URLS\_SUMMARY}} |

# Methodology

1. Browsing all the URLs on each website provided by respective Agencies

2. Identifying the list of websites per Agency having payment options

Discovery

1. Identifying if the websites have payment options and are accepting cards and are redirecting to a PCI-certified third-party payment processor (PCI-Compliant)

2. Identifying the websites having payment options and accepting card details on the same website with (non-PCI certified) or without a redirect. (Non-Compliant)

Determining Compliance

1. Reporting the status per agency/URL with the date of verification, compliance status and a screenshot of the payment page (Wherever applicable)

Reporting

# Audit Summary

The observations are made under various categories in the following order:

(A) Number of URLs provided, (B) Number of URLs with Error\*, (C) Number of URLs with Log-In Issue\*\*, (D) Number of Accessible Sites, (E) Number of URLs without pay portal, (F) Number of URLs with pay portal and their PCI status as (G) Compliant/(H) Non-Compliant/(I) Need Clarification from Agency\*\*\* (see footnotes below for an explanation of column B, C, and I).

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Agency** | **(A)** | **BREAK OUT OF URLS** | | | | | | | |
| **Number of URLs provided** | **(B)** | **(C)** | **(D) = A-B-C** | **(E)** | **(F) = G+H+I** | **PCI Status** | | |
| **\*Error** | **\*\*Log-in issue** | **(D) = E+F** | **Without pay portal** | **With pay portal** |
| **Accessible sites** | **(G)** | **(H)** | **(I)** |
| **Compliant** | **Non-compliant** | **\*\*\*Need clarification from Agency** |
| **LB** | **{{NUMBER\_OF\_URLS\_SUMMARY}}** | **--** | **--** | **{{ACCESSIBLE\_URLS\_SUMMARY}}** | **{{URLS\_WITHOUT\_PAY\_PORTAL\_SUMMARY}}** | **{{URLS\_WITH\_PAY\_PORTAL\_SUMMARY}}** | **{{COMPLAINT\_URLS\_SUMMARY}}** | **{{NON\_COMPLAINT\_URLS\_SUMMARY}}** | **{{NEED\_CLARIFICATION\_FROM\_AGENCY}}** |

**\*\* Log-In Issue "Username - Password Required; Login Credential Required; Business details are required to login; Credentials required to create a new account; Employee FEIN Account number to proceed; required Valid Routing and Account Number: Login to authorized persons only; Brand Master Info required, Invoice Number/Payment Code Required; etc."**

**\*\*\* Need clarification from Agency. There are third-party website links on the Agency’s website. These third-party websites have options to accept payment cards. The respective Agency will be contacted to provide more clarity in order to identify if the third-party websites are part of the Agency or managed by the Agency. Based on the response, the compliance status of the URL(s) will be decided.**

**\* Error Message - Error "403 Forbidden. Access is denied; Blank Page; Trouble finding that site; Forbidden; Error 401; HTTP Error 404; Session Expired; The Connection has timed out; This site cannot be reached; 404-File or Directory not found; Website Unavailable".**

**OBSERVATIONS:**

Out of number\_of\_urls URLs shary the Agency,

{{OBSERVATIONS}}

## Detailed Report

The report contains the details in the order below.

* Consolidated table for each Agency with the details of each URL and the respective audit observations
* Payment Option Available or not? If available, whether the payment link is certified by PCI DSS or not? (Screengrabs provided)
* Payment Option available but leading to 3rd Party payment URL (which needs clarification from the Agency)
* URLs which have access errors (screengrabs provided - action required from the Agency)
* URLs which have login issues (screengrabs provided - action required from the Agency)

{{DETAILED\_REPORT\_TABLE}}

{{PCI\_CERTIFIED\_SITES\_DETAILS}}

{{CLARIFICATION\_NEEDED\_SITES\_DETAILS}}

{{ACCESS\_ERROR\_SITES\_DETAILS}}

{{LOGIN\_ERROR\_SITES\_DETAILS}}

## Use of This Report

State of New Mexico Agencies, hereinafter referred to as "Client," agrees that this report provided by Securin Inc. (SECURIN), in connection with the services provided by SECURIN, and the "Client Reports" are solely for the use of the Client and its officers, directors, and employees (collectively with the Client, the "Client Entities").

Aside from the Client Entities, the Client Reports may be provided only in their entirety (unless SECURIN otherwise agrees in writing) to the auditors, legal counsel, regulators, or other parties who are under contract with the Client for the Client to provide products or services to such parties, provided that each such person or entity agree in writing to keep the contents of Client Reports confidential and not disclose this report or the information herein to others.

The client shall own all right, title, and interest in and to any written summaries, reports, analyses, and findings or other information or documentation prepared for the Client in connection with SECURIN's provision of the Consulting Services to the Client (the "Client Reports").

The provision by the Client of any Client Report or any information therein to any unaffiliated third party shall not entitle such third party to rely on the Client Report or the contents thereof in any manner or for any purpose whatsoever, and SECURIN specifically disclaims all liability for any damages whatsoever (whether foreseen, unforeseen, direct, indirect, consequential, incidental, special, exemplary, or punitive) arising from or related to reliance by any third party on any Client Report or any contents thereof.

Due to the sensitive nature of the information herein, the distribution of this report should be controlled, and the report not photocopied.

**Securin.**

A picture containing background pattern

Description automatically generated

**Securin Inc.**

**2440 Louisiana Blvd. NE Suite 560**

**Albuquerque, 87110**

**United States**