



PAYMENT CARD INCIDENT REPORT

I. EXECUTIVE SUMMARY

Describe the incident. Include the following information when possible: Date of when forensic company was engaged, Date(s) of forensic investigation, A brief summary of the environment reviewed, Cause/suspected cause of intrusion, Type of account information at risk (i.e. Cardholder name, address, account number, expiration date, CVV, PIN blocks, etc.)

TYPE OF ACCOUNT INFORMATION CONSIDERED TO BE AT RISK (Check all that apply):

- Cardholder Name Cardholder Address Primary Account Number Expiration Date
- Card Validation Value/Code PIN Blocks Service Code Social Security Number
- Other Cardholder Data (Please specify):

NUMBER OF ACCOUNTS CONSIDERED TO BE AT RISK:

TIME FRAME OF ACCOUNTS CONSIDERED TO BE AT RISK:

II. BACKGROUND

California State University, Long Beach (CSULB) is a large urban, comprehensive university in the 23-campus California State University system. Over 35,000 students attend CSU, Long Beach and approximately 2,000 student live in campus residence halls.

III. COMPLIANCE STATUS

Based on findings, the compliance status for each of the twelve basic requirements of the Payment Card Industry Data Security Standard follows:

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD		
Requirements	In Place	Not in Place
Build and Maintain a Secure Network		
Requirement 1: Install and maintain a firewall configuration to protect cardholder data	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	<input type="checkbox"/>	<input type="checkbox"/>
Protect Cardholder Data		
Requirement 3: Protect stored cardholder data	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 4: Encrypt transmission of cardholder data across open, public networks	<input type="checkbox"/>	<input type="checkbox"/>
Maintain a Vulnerability Management Program		
Requirement 5: Use and regularly update anti-virus software	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 6: Develop and maintain secure systems and applications	<input type="checkbox"/>	<input type="checkbox"/>
Implement Strong Access Control Measures		
Requirement 7: Restrict access to cardholder data by business need-to-know	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 8: Assign a unique ID to each person with computer access	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 9: Restrict physical access to cardholder data	<input type="checkbox"/>	<input type="checkbox"/>
Regularly Monitor and Test Networks		
Requirement 10: Track and monitor all access to network resources and cardholder data	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 11: Regularly test security systems and processes	<input type="checkbox"/>	<input type="checkbox"/>
Requirement 12: Maintain a policy that addresses information security	<input type="checkbox"/>	<input type="checkbox"/>

Notes:

IV. NETWORK INFRASTRUCTURE OVERVIEW

Attach a diagram of the network that includes the following:

1. Cardholder data sent to university server or data center.
2. Upstream connection to third-party processor.
3. Connection to member.
4. Remote access connection by third-party vendors of internal staff.

V. INVESTIGATIVE PROCEDURES

Describe the Response Events. Include forensic tools used during investigation:

VI. FINDINGS

1. Provide specifics on firewall, infrastructure, host, and personnel findings.

2. Identify any data exported by intruder.

3. If no hacker utilities/tools were found, explain how intrusion could occur.

4. Identify any third-party payment application, including product version.

VII. ACTIONS

Identify actions made to contain the incident. Include any dates of completion.

VIII. RECOMMENDATIONS

IX. CONTACT(S) AT CSULB AND SECURITY ASSESSOR PERFORMING INVESTIGATION

CSULB CONTACT INFORMATION:

California State University, Long Beach
1250 Bellflower Boulevard, SRM-104
Long Beach, CA 90840-5702

Last Name	First	Position	Email	Phone
Rozanski	Maryann	Information Security Officer	mrozansk@csulb.edu	562-985-8620
Wohlgezogen	Gene	Assistant Information Security Officer	gwohlgez@csulb.edu	562-985-4862

SECURITY ASSESSOR CONTACT INFORMATION:

Last Name	First	Position	Email	Phone
-----------	-------	----------	-------	-------
