

Incident Response Plan

1. In the event of a breach in card data security take the following steps:

The unit shall immediately contain and limit the exposure of cardholder data, alert Controller's Division and conduct a thorough investigation of the suspected loss or theft of account information.

- Do not access or alter compromised systems (e.g., do not log on or change passwords; do not log in as ROOT).
- Do not turn off the compromised machine. Instead, isolate compromised systems from the network (e.g., unplug the cable).
- Preserve logs and electronic evidence.
- Log all actions taken.
- If using a wireless network, change the Service Set Identifier (SSID) on the Access Points (AP) and other machines that may be using this connection (with the exception of any systems believed to be compromised).
- Be on high alert and monitor all systems with cardholder data.
- Provide Controller's Division with a report containing: account information at risk and the source and timeframe of the compromise.

Controller's Division will alert all necessary parties immediately.

NOTE: If an incident occurs during normal business hours (8:00AM to 5:00PM), notify the Office of the State Treasurer (OST) by using the number listed below. OST will then notify U.S. Bank, and coordinate all communication. If an incident occurs outside of normal business hours, contact U.S. Bank directly by using the phone number listed below.

- Internal Information Security group and Incident Response Team.
Controller's Division: VC Finance and Administration and Controller, Director Treasury Operations.
- **Office of the State Treasurer (OST); (503) 378-4000.** Notify the receptionist that you have experienced a merchant card breach, and ask to speak with the Merchant Bank Liaison on the Banking Team or a member of the Relationship Management Services team.
- **U.S. Bank; 1(800) 725-1243.** Identify that you are a "National Account" under State of Oregon, and provide them with your **Merchant ID (MID) #**. Notify the U.S. Bank customer service representative that you have experienced a merchant card breach, and ask that the incident be reported to the Risk Department.

Complete the attached Incident Report as soon as possible. This must be completed within three business days, and provided to the Office of the State Treasurer. OST will forward it to U.S. Bank/NOVA. Visa and U.S. Bank/NOVA will determine and notify the agency and OST if an independent forensic investigation, compliance questionnaire, and vulnerability scan are required.

INCIDENT REPORT

In the event of a possible credit card data compromise, complete the following information for NOVA Information Systems.

Merchant Name:

Merchant ID #:

Date of Incident:

Bank Use Only:

MCC:

BIN/ICA:

What is the transaction date range associated with the compromise accounts?

What credit card data was compromised?

Was your system storing track 1 or track 2 data?

Was your system storing CVV/CVC 2 data?

How many credit cards were involved?

Was law enforcement notified, and if so, which department/agency?

What steps have been taken to remediate the risk/vulnerabilities?

How did the compromise occur?

What are the compromised systems?

Has all possible evidence been preserved?

What software and what version are you running?

Are you PCI Compliant?

Actions Taken:

Actions Pending:

Contact Information: