

## 9.0 Information Security Compromises

Members, service providers or merchants must immediately report the suspected or confirmed loss or theft of any material or records that contain Visa cardholder data.

If a member knows or suspects a security breach with a merchant or service provider, the member must take immediate action to investigate the incident and limit the exposure of cardholder data.

If a Visa member fails to immediately notify Visa USA Fraud Control of the suspected or confirmed loss or theft of any Visa transaction information, the member will be subject to a penalty of \$100,000 per incident.

Members are subject to fines, up to \$500,000 per incident, for any merchant or service provider that is compromised and not compliant at the time of the incident.

### 9.01 In the event of a security intrusion:

- If after business hours, contact the Office of Public Safety immediately at extension 7777
- If during business hours, contact Emergency Response Team immediately, and Finance will work with Information Technology, the acquiring merchant bank, third party providers and Public Safety as necessary. See **Appendix E** for Emergency Response Team Departments and current contacts.
- Contain and limit exposure:
  - 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 SSID on the 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 Visa systems.

## APPENDIX E

### Department

### Departmental Contacts

Finance

Steven Heath	x7594	<a href="mailto:treasury@sandiego.edu">treasury@sandiego.edu</a>
Ginny Proctor	x2434	<a href="mailto:compliance@sandiego.edu">compliance@sandiego.edu</a>

ITS

Network Infrastructure Systems & Service, including CASHNet,  
[help@sandiego.edu](mailto:help@sandiego.edu)  
iModules/Blackbaud Sphere, [crm@sandiego.edu](mailto:crm@sandiego.edu)  
Micros, CBORD, Nebraska, Shift4 [auxts@sandiego.edu](mailto:auxts@sandiego.edu)

Public Safety

All systems, during non-business hours 619-260-7777

Acquiring Merchant Bank

Patty White [Patty.White@wellsfargo.com](mailto:Patty.White@wellsfargo.com)