Credit Card Acceptance Policy

Background and Purpose

Alternatives to Violence acceptance of credit cards to pay for donations, tickets for fundraising events, and other fundraiser payments has been growing over the past several years. Increased interest in accepting payments over the Internet (eCommerce) has also grown, spurring the need to establish business processes and policies that protect the interests of Alternatives to Violence and its donors.

In order to ensure that credit card activities are consistent, efficient and secure, Alternatives to Violence has adopted the following policy and supporting procedures for all types of credit card activity transacted in-person, over the phone, via fax, mail or the Internet. This policy provides guidance so that credit card acceptance and eCommerce processes comply with the Payment Card Industry Data Security Standards (PCI DSS) and are appropriately integrated with the Alternatives to Violence's financial and other systems.

Security breaches can result in serious consequences for Alternatives to Violence, including release of confidential information, damage to reputation, added compliance costs, the assessment of substantial fines, possible legal liability and the potential loss of the ability to accept credit card payments.

Applicability

Any Alternatives to Violence employee, contractor or volunteer who, in the course of doing business on behalf of Alternatives to Violence, is involved in the acceptance of credit card and eCommerce payments for Alternatives to Violence is subject to this policy.

Policy Statement

All Employees must:

1. Ensure that all employees, contractors and volunteers with access to payment card data acknowledge in writing that they have read and understood this Policy for Accepting Credit Card and eCommerce Payments. These acknowledgements should be submitted, as requested, to the financial manager to be included in their personnel file.

2. Ensure that all credit card data collected by the employee regardless of how the payment card data is stored (physically or electronically, including but not limited to account numbers, card imprints, and Terminal Identification Numbers (TIDs)) is secured. Data is considered to be secured only if the following criteria are met:

- Only those with a need-to-know are granted access to credit card and electronic payment data.
- Email should not be used to transmit credit card or personal payment information.
- Credit card or personal payment information is never downloaded onto any portable devices such as USB flash drives, compact disks, laptop computers or personal digital assistants.
- Alternatives to Violence does not accept fax transmissions (both sending and receiving) for credit card payments.
- The processing and storage of personally identifiable credit card or payment information on Alternatives to Violence computers and server is prohibited.
- The three-digit card-validation code printed on the signature panel of a credit card is never stored in any form.
- The full contents of any track from the magnetic stripe (on the back of a credit card, in a chip, etc.) are never stored in any form.
- All media containing credit card and personal payment data that is no longer deemed necessary or appropriate to store are destroyed or rendered unreadable.

No Alternatives to Violence employee, contractor or volunteer who obtains access to payment card or other personal payment information in the course of conducting business on behalf of Alternatives to Violence may sell, purchase, provide, or exchange said information in any form including but not limited to imprinted sales slips, carbon copies of imprinted sales slips, mailing lists, tapes, or other media obtained by reason of a card transaction to any third party other than to Alternatives to Violence's acquiring bank, depository bank, Visa, MasterCard or other credit card company, or pursuant to a government request.

Process to Implement Acceptance of Credit Card

Credit Card donations are accepted through our website alternativestoviolence.org which uses Paypal as our merchant vendor. Alternatives to Violence uses QuickBooks credit card system. The payment or donation can be entered into Quickbooks and processed. Any credit card information that is written down should then be destroyed. Alternatives to Violence also accepts credit card donations through First Bank. For events, First Bank loans their credit card machines to us. We use the machines at the event and return them afterwards. For the above two methods no credit card numbers should be kept or stored by Alternatives to Violence. Occasionally, Alternatives to Violence uses a manual machine and slips to accept credit card payments. These payments are processed by phone through First Bank. After the slips are created they should be stored in a locked box or storage unit. Once the credit card amount has cleared the bank the slips should be shredded so that they are unreadable. If the credit card

slips need to be transported they should be transported by Alternatives to Violence personnel and kept in the locked box until they are received in the office.

Process for Responding to a Security Breach

In the event of a breach or suspected breach of security, Alternatives to Violence must immediately execute each of the relevant steps detailed below.

1. Employees should notify the Executive Director of an actual breach or suspected breach of credit card information. Email or phone should be used for initial notification and to provide a telephone number for the Executive Director to call in response. Details of the breach should not be disclosed in email correspondence.
2. The Executive Director or any individual suspecting a security breach involving eCommerce also must immediately ensure that the following steps, where relevant, are taken to contain and limit the exposure of the breach:

    - Prevent any further access to or alteration of the compromised system(s). (i.e., do not log on at all to the machine and/or change passwords; do not log in with ROOT or Administrative authority.)

    - Do not switch off the compromised machine; instead, isolate the compromised system(s) from the network by unplugging the network connection cable.

    - Preserve logs and electronic evidence.

    - Log all actions taken..

3. The Executive Director should call the merchant bank and the Police Department.

4. At the relevant credit card associations' request and depending on the level of risk and data elements compromised, the Executive Director in conjunction with the Police Department shall, within 4 business days of the event:
    - Arrange for an independent forensic review.
    - Arrange for a network and system vulnerability scan.
    - Complete a compliance questionnaire and submit it to relevant card association(s).

Ongoing Policy Management

- Alternatives to Violence may modify this policy from time to time as required, provided that all modifications are consistent with Payment Card Industry Data Security Standards then in effect.

- The Executive Director is responsible for initiating and overseeing an annual review of this Policy, making appropriate revisions and updates and issuing the revised policy to appropriate personnel.