Elavon

# Data Compromise Management

## What is a Data Compromise Event?

Simply stated, a data compromise event is unauthorized access to and illegal theft of payment card data. A central target for a data compromise event is often credit or debit card information which a perpetrator will typically re-sell or use in the production and presenting of counterfeit cards. There are three basic types of data compromise events:

- **Physical Theft.** Stealing receipts, hardware or other documentation which contains card data
- **Skimming.** Theft of card information used in an otherwise legitimate transaction
  - Typically an "inside job" by a dishonest employee of a legitimate merchant
  - The thief can procure a victim's card number using basic methods such as photocopying receipts or more advanced methods such as using a small electronic device (skimmer) to swipe and store a victim's card magnetic stripe information
- **Systemic Intrusion.** Utilizing malicious, unauthorized and illegal means to obtain electronic access to payment processing systems or storage mediums, often referred to as hacking

## What to do if Compromised

### 1. Immediate containment

- Do NOT access or alter compromised systems (i.e., do not log on at all to the machine and change passwords, and do not log in as ROOT)
- Isolate compromised systems(s) from the network (i.e., unplug network cable). Do not turn the compromised system(s) off.
- Preserve all merchant logs and electronic evidence
- Make a record of all action taken, who took the action and the date and time of such action
- If using a wireless network and a compromise is suspected, disable the wireless network
- Monitor all systems with cardholder data for possible threats or issues

### 2. Alert all necessary parties immediately

- Merchant internal security group at our partner, Elavon:
  - 865.403.7321 (Amanda Duggin)
  - 865.403.8852 (Chris Geron)
- Law enforcement
- Check applicable state laws for possible notification to cardholders

**3. Follow-up with Elavon.** We will send you a questionnaire either by e-mail or facsimile which must be completed and returned to us within 3 calendar days. This information may be forwarded to the card brands as part of the investigation process. You will need to provide us with the transaction information that was possibly involved in the data compromise within 7 calendar days so that the information can be provided to the card brands. We will assist with determining what information must be reported.

**4. Determination of need for independent forensic investigation.** The Card Brand(s), in consultation with Elavon, will determine whether an independent forensic investigation will be required. Approved forensic investigations may be required to:

- Assess a compromised entity's computing environment to identify relevant sources of electronic evidence
- Assess all external connectivity points within each location involved

- Assess network access controls between compromised system(s) and adjacent and surrounding networks
- Acquire electronic evidence from compromised entity's host and network based systems
- Forensically examine electronic evidence to find cardholder data and establish an understanding of how a compromise may have occurred
- Verify cardholder data is no longer at risk and/or has been removed from the environment
- Present forensic investigation findings to the relevant parties involved in the incident

5. **Merchant to ensure all PCI/DSS requirements are met.** All merchants are expected to be compliant with applicable PCI/DSS guidelines. PCI/DSS is a set of comprehensive requirements for enhancing payment account data security and was developed by the founding payment brands of the PCI Security Standards Council (PCI/SSC), including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., to help facilitate the broad adoption of consistent data security measures on a global basis. PCI/DSS is a multifaceted security standard that includes requirements for:
   - Security management
   - Policies
   - Procedures
   - Network Architecture
   - Software design
6. **Demonstrate PCI/DSS compliance to the card brands.** Once the merchant meets the appropriate requirements for PCI/DSS compliance, we will assist the merchant in demonstrating full compliance to the card brands. Merchant point of contact at our partner, Elavon will be Amanda Duggin who can be contacted at 865.403.7321 or via email at Amanda.Duggin@elavon.com.

   To demonstrate full PCI/DSS Compliance to the card brands:
   - Upgrade to a validated payment application (if applicable).
   - For a list of PABP-compliant payment applications please visit www.pcisecuritystandards.org/approved_companies_providers/index.php

## Contact Information at our partner, Elavon

E-mail: #ADCQueries-NA@elavon.com

7300 Chapman Highway
Knoxville, TN 37920 USA

Chris Geron, Vice President
Phone: 865.403.8852
E-mail: Chris.Geron@elavon.com

Amanda Duggin, Data Compromise Coordinator
Phone: 865.403.7321
Email: Amanda.Duggin@elavon.com