MasterCard Worldwide

Account Data Compromise Management

Best Practices Framework For Issuers and Acquirers

PCI Best Practices

THE NUMBER OF AMERICANS IMPACTED BY DATA BREACHES INCREASED BY 67% BETWEEN 2010 AND 2011 AND THESE SAME VICTIMS WERE 9.5 TIMES MORE LIKELY TO BE A VICTIM OF IDENTITY FRAUD THAN CONSUMERS WHO WERE NOT AFFECTED BY A DATA BREACH EVENT.

Best Practices Framework For Issuers and Acquirers

MasterCard's issuing and acquiring customers know that account data compromise (ADC) events can be a significant cost of doing business in an age where hackers use sophisticated technology to execute cyber attacks from anywhere in the world.

However, despite the various opportunities attackers have to exploit vulnerabilities and compromise payment data, financial institutions can — and should — ensure that they are employing the most appropriate mix of tools and resources they can to prevent, detect, and respond to these ongoing ADC threats.

Impact of ADC Events

ADC events have potentially far-reaching consequences for financial institutions beyond the obvious financial ones. According to a 2012 Javelin report[1], the number of Americans impacted by data breaches increased by 67% between 2010 and 2011. In addition, these same victims were 9.5 times more likely to be a victim of identity fraud than consumers who were not affected by a data breach event. Media coverage of data breaches often stresses the link between data breaches and identity "theft", exposing financial institutions to increased reputational risk and a negative impact to customer loyalty.

Beyond the impact to reputation or customer loyalty, the financial cost of a data breach is quite significant. For example, a 2012 Symantec Corporation and Ponemon Institute study[2] concluded during its review of 49 data breach events last year that the organizational cost of a data breach was $5.5 million, or $194 per compromised record. The same study also stressed the importance of organizational factors in reducing that cost. For example, having a CISO with overall responsibility for enterprise data protection could reduce the cost per compromised record by as much as $80. Employing outside consultants to assist with breach response can also save as much as $41 per compromised record. Research shows that efforts made by issuers, acquirers and their customers to mitigate and quickly remedy a breach event have a positive impact on the bottom line.

When factoring in both the hard dollar costs and the reputational fallout following an ADC event, all the signs clearly show that issuers and acquirers need to focus on the key fundamentals of ADC event management as part of their regular business activities.

1 Javelin Strategy & Research; dentity Fraud Report. February 2012
2 Symantec Corp. and Ponemon Institute 2011 Cost of Data Breach Study: United States. March

CONTINUED FROM COVER

ADC Event Management Best Practices

MasterCard recommends that issuers and acquirers consider the following best practice framework when determining how to manage future ADC events:

- End-to-End Event Management
- Proactive Data Security and Education
- Risk Communications Guidelines

End-to-End Event Management

All ADC events have a lifecycle that includes pre-, during, and post-breach activities. It is critical that issuers and acquirers understand this lifecycle as it specifically relates to their current business operations and strategic planning efforts.

For issuers, effective end-to-end event management should entail:

- Establishing an operations plan that determines cross-departmental product impacts and identifies the capabilities of the organization's functional units to address ADC events
- Determining effective risk matrices for all ADC events to assist in proper business decisions concerning monitoring and re-issuance of accounts based on risk levels
- Establishing detection methodologies to proactively identify potential Common Points of Purchase (CPP)
- Diligent and comprehensive reporting of data accounts that have been compromised, including fraud status codes, into MasterCard's System to Avoid Fraud Effectively (SAFE) database

For acquirers, effective end-to-end event management should entail:

- Establishing an operations plan that includes ADC event severity matrix rating protocols
- Creating a core incident response team consisting of cross-functional management groups
- Methodology to assist the payment brands with outreach to the breached entity and the commitment to stay engaged during the entire ADC event lifecycle

Proactive Data Security and Education

Both issuers and acquirers must be committed to helping educate and reinforce appropriate data security practices to their customers, whether they are cardholders, merchants, Third-Party Processors, or other types of Data Storage Entities and Data Providers.

- Often, savvy cardholders are the first line of defense when it comes to preventing their payment accounts from being compromised; therefore, issuers should focus on cardholder education by:
  - *Recommending cardholders review their payment card statements often*
  - *Providing information about popular fraud scams, such as phishing and skimming*
  - *Promoting the use of online protection measures, such as anti-virus, anti-spyware, and firewall software*
  - *Offering tips on what to do if customers believe they are the victim of an ADC or identity theft event*
  - *Providing elements of what makes a strong online password*
  - *encouraging cardholders to report suspected ADC events to their issuer*
- Acquirers also need to ensure that they are doing all they can to protect the integrity of payment card account data, including:
  - *Educating value chain partners such as merchants and processors about what types of sensitive payment card data can and cannot be stored*
  - *Establishing an effective Payment Card Industry Data Security Standard (PCI DSS) program to drive merchant compliance. MasterCard's acquiring partners can leverage the MasterCard Merchant Education Program to support PCI compliance training activities for merchants (www.mastercard.com/us/merchant/support/merchant_education.html)*
  - *Sharing information about known security vulnerabilities of software and payment devices that have led to past data compromises*

Risk Communications Guidelines

During a data breach event, most organizations struggle to keep up with the demand for information from various stakeholders. The pressure of knowing what to say and to whom can be reduced by developing a risk communications strategy before an ADC event occurs. Elements of a tested ADC event communications response framework should include:

- A dedicated ADC event communications response team that includes members who have direct interactions with all the stakeholders that may be affected by a breach event
- An ADC event communications plan that includes checklists for response activities based on triggers or event timing, contact information for all team members, and template response materials that include "evergreen" messaging that has been vetted by the response team and legal counsel
- A stakeholder communications matrix that matches key audiences against internal and external communications channels, delivery dates, and the internal staff responsible for disseminating the messages

During an ADC event, consider the following:

- Use simple language without industry jargon
- Rely on facts, not speculation
- Express empathy for affected audiences and inform them what to do to mitigate any possible negative impact of an ADC event
- Share information regarding what actions are being taken to protect customers
- Incorporate, when possible, zero liability language into cardholder response materials to help address financial impact concerns

MasterCard Worldwide