

Data Security and Privacy: Into the Breach

Martha Lessman Katz, JD, CIPP, CLP

Martha Lessman Katz, JD, CIPP, CLP, is a principal at Miles & Stockbridge PC in Baltimore, Maryland.

In 2007, an attack against the computer systems of the TJX Co. potentially exposed credit card and other personal information of 45 million T.J. Maxx customers. The 2008 intrusion into Heartland Payment Systems' processing system—the fifth largest in the United States—compromised more than 100 million credit and debit card transactions.

And in an ignominious end to 2009, a malicious attack against RockYou.com's user database compromised the user names, passwords, and e-mail addresses of more than 32 million account holders.

Stolen confidential business and personal information may be disseminated over the Internet in a matter of minutes. Even if personal data are not compromised, the loss of even one computer may mire an institution in a tangled web of international data security and privacy laws and regulations. And the resulting financial cost pales when compared to the damage to reputation, customer wrath, and loss of trust.² Still, rarely a day goes by without a data breach being reported by an academic institution, health-care organization, or other business or government agency.