ASM Educational Center (ASM) *Est. 1992*

11200 Rockville Pike, Suite 220 Rockville, MD 20852 | **Phone**: 301-984-7400 | **Fax**: 301-984-7401
Web: www.asmed.com | **E-mail**: info@asmed.com

E-Commerce & Online payments Sector

Source: Deloitte Report

Case 3

Thieves use stolen data to create their own credit cards

Organization
A large financial services firms that provides electronic transaction processing worldwide.

Scenario
A group of criminals broke into the company's systems and over the course of a year stole magnetic stripe data for approximately 7 million credit cards. They then created fake credit cards by programming the stolen data onto cheap prepaid cards, which were later used to purchase expensive items such as computers and televisions.

Attackers and motivation
The attackers were motivated by financial gain. The careful target selection and sophisticated techniques used for the attack suggest the involvement of a well organized cyber-criminal group.

Techniques used
Attackers infiltrated a crucial part of the payment processing infrastructure containing magnetic stripe data, which was then exported to create duplicate credit cards that were later used for fraudulent transactions.

Business impact
The company revealed that the data breach cost an estimated $90 million, which includes fraud losses as well as fines, costs associated with the investigation, charges from card networks and client aftercare. The company's reputation also took a lot of damage, both from consumers and from clients within the payment card networks.