# Adobe Data Breach Case Study

## Introduction

Name of Case: Adobe Data Breach  
Date of Case: October 2013  
Link: https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/

## Why Did This Case Make the News?

The Adobe breach gained widespread attention due to the sheer number of affected users—over 153 million. Initially reported as affecting 3 million customers, the scope rapidly expanded, exposing encrypted credit card records, usernames, and hashed passwords. The breach highlighted major security oversights by a major tech company and sparked lawsuits, legal settlements, and industry scrutiny.

## Describe the Breach

The breach involved a combination of unauthorized access and data exfiltration. Hackers gained access to Adobe’s systems, stealing source code for numerous Adobe products and a database containing encrypted customer information. The exposed data included usernames, encrypted passwords, email addresses, and credit/debit card information.

## Why Was This Company a Target?

Adobe was a lucrative target due to the valuable software it develops and the massive amount of user data it collects. Its broad customer base, including individuals and corporations, made it attractive for cybercriminals seeking sensitive data.

## Identify the Threat(s)

Immediate Threat(s): Theft of personal and financial information including login credentials and credit card data.  
Potential Threat(s): Long-term risk of identity theft, credential stuffing, and fraud if data was reused or decrypted.

## What Could a Developer Have Done to Prevent This Breach?

- Regularly update and patch systems to close vulnerabilities.  
- Use strong encryption and salting methods for passwords.  
- Implement intrusion detection systems (IDS) and conduct frequent security audits.  
- Apply the principle of least privilege to limit internal access to sensitive data.

## Which Policy or Policies Will Help Prevent This Type of Attack?

- GDPR / Data Protection policies  
- Secure Software Development Lifecycle (SSDLC)  
- Regular Penetration Testing and Vulnerability Assessments  
- Incident Response and Governance Protocols

## Summary: Role of Best Practices, AAA, and Defense in Depth

Best practices such as secure coding, proactive monitoring, and layered defenses are essential to preventing breaches. Authentication (e.g., multi-factor login), Authorization (e.g., access control restrictions), and Accounting (e.g., logging and auditing access) can help track and limit unauthorized activity. Adobe’s case demonstrates a lapse in the ‘Defense in Depth’ model—specifically in application and data layer protections—where strong practices at each layer could have reduced the scale of the breach.