



4600 Montgomery Road, Suite 400

Cincinnati, OH 45212

Phone 513.841.5000

Fax 513.841.5072

Epsilon Breach: Frequently Asked Questions

Justin Hall, CBTS Information Security

Published on April 7, 2011

Who is Epsilon?

Epsilon is a subsidiary of Alliance Data Systems that offers marketing services to thousands of organizations. A significant portion of these services revolve around email-based marketing. Epsilon business customers, such as Kroger, Tivo, Hilton Hotels, and Citigroup, provide Epsilon with email addresses from their own customers that sign up to receive marketing email, and Epsilon creates and delivers email content to them. ^[1]

What happened?

On March 30, an attacker obtained unauthorized access to some of Epsilon's business customer data. This data consists of the names and email addresses provided by Epsilon's business customers to receive email marketing. ^[2]

How many were affected?

While only a few dozen of Epsilon's thousands of business customers were affected, the number of records stolen could number in the millions, considering the significant size of the businesses that reported the breach to their customers. ^[3]

Why would someone steal this data?

Email lists are valuable to spammers, whose goal is to reach as broad an audience as possible with their unsolicited content. We can also assume the lists are tied to the business customers who provided them to Epsilon – meaning an attacker could send fraudulent email to the customers, acting as if they originated from the business customer themselves. The recipient would likely feel safer opening the email and following any instructions it provided, if they are used to receiving email from that business.

What's the worst-case scenario?

A targeted phishing attack. An attacker could send an email to an individual on a bank's customer list, and design the email so that it is convincing as a legitimate message. This message could claim that, due to the Epsilon breach, it was discovered that the user's online banking credentials or personal financial data was also compromised, and direct the user to change their online banking credentials immediately. The email could then point the user to a fraudulent website, appearing to be hosted by the bank itself, and provide a form where the user could supply their existing credentials, or financial information, allowing them to be stolen by the attacker.

This kind of attack is possible for any business customer of Epsilon's where the business customer is responsible for customer data – any number of scenarios arise where attackers could coerce the customer to a fraudulent website to supply sensitive information.

How can we protect ourselves from a similar attack?

Begin with a data classification exercise. Identify all types of data for which your organization is the primary owner, or a steward. Examples of primary ownership include internal company information, employee personal data, customer usernames & passwords, or customer account numbers. Data for which you are a steward includes customer personal information, such as name, address, phone, social security number, or financial data, such as account numbers or credit card numbers.

Establish internal owners of each category of data. Define secure storage, data retention requirements, and destruction mandates for each category. Establish access controls that only allow access to read, modify, and delete the data by authorized users and systems. Monitor access to the data at the storage point, and investigate suspicious activity. Monitor perimeter activity, using a data leakage prevention product, to identify when sensitive data is leaving your network.

Be aware of other organizations – vendors, customers, government entities, and so on – that may steward your data. Make sure they provide you with copies of their policies that dictate how they will and will not use your data. Ensure they take sufficient measures to protect your data.

Educate users and customers about modern attack techniques. Warn them to be wary of any email-based communication that asks them to provide or change sensitive information – such as usernames and passwords, account numbers, social security numbers, etc. Advise against clicking links or opening attachments in email messages – instead, direct them to manually browse to websites to ensure they are visiting an authentic site.

[1] <http://www.epsilon.com>

[2] <http://www.securityweek.com/massive-breach-epsilon-compromises-customer-lists-major-brands>

[3] <http://phx.corporate-ir.net/phoenix.zhtml?c=120991&p=irol-newsArticle&ID=1547436&highlight=>