

Debix Case Studies: A Tale of Two Breaches

Case Study #1

The Customer

This large national healthcare company provides treatment throughout the US. This company reported annual revenue in excess of \$3 billion in 2007.

The Challenge

While this company did not experience a large-scale breach, it has been subject to multiple incidences of data compromise occurring on a smaller scale, as is typical with most large companies managing thousands of customer records. Smaller compromises were discovered during the company's regular due diligence of tracking lost or stolen devices (laptops, USB drives and PDAs), lost or missing paper files, and assessing damage following physical break-ins at company locations. The company began doing case-by-case assessment of the facts each time an incident was detected, carefully determining whether the potentially exposed information could cause harm to the customer from the perspective of identity theft.

"Now there's been a shift in consumer expectations, in terms of what the owner of the data will actually do if the data is breached"

– Chief Security Officer, Large National Healthcare Company

In one particular incident, the exposed data was identified as highly sensitive, involving social security numbers. The company notified these individuals, described the situation and the information that had been compromised. Upon receiving the breach notification letter, several customers called the company, inquiring what action was going to be taken.

The Solution, Implementation and the Result

The company had already begun researching different solutions offered to breach victims, but after comparing the Debix solution to credit monitoring, the company quickly chose Debix because of its fraud preventative capability. It was the company's desire to provide a preventative solution rather than reactive product for the best financial value, with Debix showing a clear advantage over other solutions. Now, notification includes a basic explanation of the breach, information about identity theft, a registration form for Debix and a description of how it can help prevent identity theft.

"Which would you prefer, a solution that stops fraud before it happens, or lets you know after the fact? It's as simple as that"

– Chief Security Officer, Large National Healthcare Company

Debix Case Studies: A Tale of Two Breaches

Since implementing the Debix Identity Protection Network, the company reports that customers appreciate the inclusion of Debix as part of its data breach response. Debix has also resonated well with the institution's business partners in breach situations requiring a collaborative response.

Case Study #2

The Customer

This company is a large healthcare corporation operating in the US. The company also manages physician practices, outpatient diagnostic clinics, and ambulatory surgery centers.

The Challenge

In 2007, the company was subject to an insider fraud attack, when it was discovered that a rogue employee had been stealing patient information to perpetrate fraud. This employee had access to the demographic information of many patients, obtained from health records (driver's license, SSN, date of birth). Using the stolen data, the employee began identifying those individuals whose personal information would be ideal for creating fraudulent new credit cards. The employee was arrested and had patient record information with him at the time of his arrest.

The Solution, Implementation and the Result

The company decided it would be best to examine every record the employee had accessed and determine which patients to notify. The patients were immediately informed of the situation. Over the period of one month, the company received seven phone calls from notified customers who suspected fraud in connection to the breach, of which five were determined to actually be fraud victims. Given the difficult nature of insider breach, the company concluded the best course of action was to provide general notification for all customers.

The company had been considering different fraud protection solutions, as it had not offered identity protection in past security breaches. The company declined the credit monitoring service option and chose Debix for its robust preventative capability and value, as other fraud alerts providers were more costly.

"The decision was straightforward: Debix provided the strongest protection at a superior value. Since implementing the Debix solution, the role of our identity theft task force in handling the customer-facing component of data breach resolution has been strengthened considerably."

– Director of Privacy and Security, Large National Healthcare Company

Debix Case Studies: A Tale of Two Breaches

In previous years, the company offered an identity protection solution only if the breach victim made an explicit request. The company has since realized that offering breach victims the opportunity to enroll in optional fraud protection was crucial for customer service. Furthermore, it was more in line with the company's new vision to provide their customers with the best possible resolution. As a result, the current Director of Privacy and Security established an Identity Theft Task Force within the company to evaluate different options for breach victims. The decision was straightforward: Debix provided the strongest protection at a superior value. Since the implementation of the Debix solution, the role of the task force in the customer-facing component of data breach resolution has been strengthened considerably.

The company highly recommends the Debix solution to other organizations and has already made the recommendation to another healthcare system that was recently breached. One of the primary reasons for the company's satisfaction with Debix solution was the rapid efficiency in which the Debix team was able to put everything together. Within 24 hours, the company had the Debix enrollment codes ready to send out to the victims, a separate site for registration, a paper enrollment form, and FAQ piece. Because there was no delay in implementation, the company was able to contact breach victims about the option to enroll by the following day.

Aside from expediting the notification process, incorporating the Debix solution in the data breach response process played a significant role in keeping incoming calls from concerned breach victims at bay. Customers were relieved that the company was taking action to manage the situation, and just knowing that they had the option to enroll in a fraud protection service provided a strong sense of comfort.