Payment fraud prevention after data breaches

by Constantin von Altrock

Highlights

Data breaches, in which card numbers of payment cards were stolen from payment processors or merchants, have resulted in substantial fraud losses over the past years. A data breach that occurred in an ATM network in India in September 2016 was reported to have also included the cards' PINs.[1] In previous data breaches, PINs were not obtained, so the stolen card data was used primarily to commit e-commerce fraud. In the case of the India breach, criminals were now also able to commit fraud at ATMs because they were in possession of the PINs. In this point of view, I discuss how the IBM Safer Payments fraud prevention solution can be used to help protect financial institutions from losses arising from such data breaches.

Protecting from financial losses

Substantial fraud losses resulting from data breaches make it apparent that higher standards of data protection are needed for every party involved in processing payment data. Despite this fact, it's expected that the number of data breaches will not decline in the immediate future. In this point of view, I focus on the protection measures that can be taken to help protect customers and payment processors from losses once a data breach occurs.

IBM Safer Payments helps protect card issuers by monitoring all authorization requests from payment transactions in real-time. If it detects that a transaction is part of a fraud scheme, it will decline the transaction before it is completed. As a result, fraud losses can actually be prevented.

In order to detect if a transaction is part of a fraud scheme, IBM Safer Payments profiles behavior over time for all entities involved in a payment. This profiling includes cardholders, ATMs, ATM network operators, terminals, and regions.

It's important to differentiate two phases:

1. The breach occurred, but it's not yet known by the payment processors, or it's not yet known what cards are affected.
2. The breach and which cards are affected is known.

Before the breach is known

Even before a payment processor knows that a breach has occurred, or is aware of what cards have been affected, IBM Safer Payments is able to detect the typical exploitation behavior of criminals. Because these data breaches typically involve a significant number of cards, an important capability of IBM Safer Payments is that it can immediately identify sudden behavioral changes for multiple cards at one time, at once.

In the India breach, for example, criminals exploited a significant number of cards in China and the US. If IBM Safer Payments had been deployed, it would have identified that:

- within a short period of time
- a significant number of ATM withdrawals were made from cards issued in India
- involving only few ATMs within the same region,
- where previous transactions indicate that the legitimate cardholder is physically located in India,
- and/or had never before traveled to the region where the ATM withdrawals occurred.

Fraudulent ATM withdrawals are often made using multiple compromised cards in a very short period of time at the same ATM, or set of ATMs, and for similar amounts. In addition, fraudulent card use frequently involves multiple withdrawals from one compromised card at the same or nearby ATMs.

When IBM Safer Payments detects such behavioral patterns, it is highly likely that the ATM withdrawal authorization requests would result in fraud. IBM Safer Payments therefore recommends to decline such requests before they are authorized. Because it is highly unlikely that this is legitimate behavior, there is a very low chance that declines would be false alarms that inconvenience legitimate cardholders.

Detecting the point of compromise

A very important aspect is that IBM Safer Payments also looks back in the history of multiple cards exposing the same fraudulent behavior for common points where they have been used in the past. In the India breach, it was reported that the card data was compromised at several ATMs of a single ATM network operator in India. IBM Safer Payments' common points analysis could have identified the set of ATMs that were used to compromise the card data and the time period in which this had taken place.

This information is useful for two purposes:

- It allows IBM Safer Payments to clearly identify all potentially compromised cards, even the ones that were not yet used to attempt fraud. It can thus scrutinize any future transaction of the compromised card even more thoroughly. For example, the first e-commerce transaction ever made from a card always carries a certain amount of risk with it. However, every card will have a first e-commerce transaction, and declining them without an additional indicator of high risk would generate massive number of false alarms. However, if IBM Safer Payments identifies that a card was used at one of the ATMs that were used to compromise card data in the time that this was occurring, and then it soon thereafter has its first e-commerce transaction (in combination with other risk factors), IBM Safer Payments can use this to securely identify a likely fraudulent transaction.
- A list of compromised ATMs as determined by IBM Safer Payments is also useful for criminal investigations. An ongoing data breach may be stopped more efficiently if authorities know which ATMs have been affected.

After the data breach is known

IBM Safer Payments can help mitigate the damage of a data breach. It can help whether it detected the breach itself and compiled the list of devices used, or whether the breach and affected cards were identified by other means. In the India breach, when the full set of affected cards is known, card issuers will ask their customers to change their PINs. Some card issuers will probably exchange their cards entirely to ensure the compromised card numbers are invalidated. Some card issuers may even block transactions of affected cards until such measures are completed.

While this is considered a necessary measure, it inconveniences many legitimate customers, and adversely impacts the reputation and brand value of the issuing banks. IBM Safer Payments provides a less disruptive approach. It will only decline transactions that are consistent with the exploitation of card data by criminals, allowing cardholders to continue to use their cards for legitimate transactions.

Had it been in place during the India breach, IBM Safer Payments could have declined fraudulent ATM withdrawals from the regions the criminals used. However, if a customer had legitimately been using his card to withdraw funds from the affected ATMs before the breach, there's a high chance of this not being fraud. Also, all other transactions occurring after the breach that involve merchants and ATMs used before the breach are likely not fraud.

With this individualized fraud prevention strategy, using IBM Safer Payments, issuers do not have to shut down all operations for cards affected by the data breach, but only decline transactions that are likely fraudulent. This can continue until the PINs are changed or the cards are replaced. In some cases, where declining the likely fraudulent transactions is enough to effectively stop the fraud, PIN changes and card replacements become unnecessary.

Summary

All over the world, measures to secure data centers and networks against card data theft are improving. However, it still must be assumed that there will be ongoing successful criminal attacks in which data is stolen and subsequently used to commit payment fraud. In this point of view, I have shown how transaction monitoring that uses behavioral profiling, and that declines likely fraudulent transactions, can not only protect from losses due to criminal attacks following data breaches, but can also minimize the negative impact on affected cardholders.

For more information

To learn more about IBM Counter Fraud Management for Safer Payments, contact your IBM representative. Or visit: **ibm.com**/saferpayments

Constantin von Altrock

Director, Counter Fraud Management

IBM Industry Solutions
Germany

constantin.von.altrock@de.ibm.com

IBM Corporation
Analytics Group
Route 100
Somers, NY 10589

Produced in the United States of America
October 2016

1 Devidutta Tripathy, *Security breach feared in up to 3.25 million Indian debit cards*, Business News, October 2016 (www.reuters.com/article/us-india-banks-fraud-idUSKCN12K0CC)

Please Recycle

FMW03026USEN-00