nintex

A rapid response to minimizing the impact of data breaches

Overview

On December 19, 2013, Minneapolis-based Target Corporation announced their customers had been victims of one of the largest credit card breaches in history. The retailer revealed that between November 27th and December 15th of that year, hackers stole nearly 40 million credit and debit card numbers using malware installed on point-of-sale (POS) machines throughout stores nationwide. Target later revised the number of compromised cards upward to 70 million.

News of the Target breach hit small and mid-sized card issuers hard. They faced the prospect of somehow manually changing card holder limit and noting accounts, then cancelling and reissuing cards. Scores of banks used data automation software to automate the entire process, performing what would otherwise be handled by a few unlucky employees over the course of a weekend, in a matter of hours.

- $500MM bank had 900 compromised debit cards in data breach.
- Needed to inform customers, note accounts, issue new cards, and "Hot Card" existing cards quickly.
- Faced with manually performing each of these steps over a series of days, or paying core provider to handle it for them.
- Utilized Automated Employees to automate the entire data breach recovery process.
- Saved significant time and money, plus ensured 100 percent accuracy, with data automation.

Organization
Banking Institution

Industry
Banking

Country
USA

About Nintex

Nintex is the global standard for process management and automation. Today more than 10,000 public and private sector organizations across 90 countries turn to the Nintex Platform to accelerate progress on their digital transformation journeys by quickly and easily managing, automating and optimizing business processes. Learn more by visiting **www.nintex.com** and experience how Nintex and its global partner network are shaping the future of Intelligent Process Automation (IPA).

Product or service names mentioned herein may be the trademarks of their respective owners.

The Challenge

The traditional recovery from a breach like this involves sending a letter and e-mail to affected customers, manually lowering transaction limits, manually updating account information, then manually cancelling and reissuing cards. One Massachusetts-based, $500 Million community bank sought to minimize their card holders' inconvenience and loss from the Target breach in another way. Three days after the Target news broke – a Friday morning – this bank still had not received a Compromised Account Management System (CAMS) alert from Visa identifying the stolen numbers. A quick account search for Target transactions during the time period in question revealed that approximately 10 percent of their card holder base (900 cards) was potentially affected by the breach.

The Nintex RPA Solution

Already a Nintex RPA customer, this bank was able to utilize the data automation software to automate the process of cancelling and reissuing compromised cards, quickly and accurately, to minimize customer downtime. "We try to reduce the customers' inconvenience, mitigate the risk associated with the fraud, and minimize the amount of interchange income we'd lose." explained the bank's Assistant Vice President of Operations Systems. "Nintex RPA helped us do all of that." Nintex RPA works like an automated employee to perform any unstructured manual task, like data entry or maintenance, automatically and with total accuracy. First, the bank identified any accounts that were both active and potentially affected by the Target breach using their data warehouse.

Nintex RPA pulled those customers' names, addresses, and other information and populated a form letter and e-mail notifying customers of the compromise. Nintex RPA then automatically performed file maintenance, changing user codes and adding notes to each affected account.

The bank next began the process of adjusting debit limits and updating user codes for each of the roughly 900 cards believed to have been compromised. Limits on ATM withdrawals remained at their usual $500 level, but PIN purchase transaction limits were lowered from $3,500 to $1,500 and signature transaction limits were set at $0. "Nintex RPA helped us manage the change in card status, the change in card limits, and the change in user code fields to identify which cards were potentially having problems." said the bank's Assistant Vice President of Operations Systems. "All of this was completed in a couple of hours."

With letters sent, accounts noted, and limits reduced, the bank began the process of automating the card issuance process with Nintex RPA. By Friday afternoon, the bank had issued new cards to 40 percent of its customer base and issued the remaining cards the following Monday. Within a week, half of all new cards had been activated. After 30 days following the incident, Nintex RPA will be used to automatically place any of the original cards that still remain active into a "hot card" status. "When something like this happens, it's not going to happen once. So we built a process and scripts so we're prepared for the next one." explained the Assistant Vice President of Operations Systems. "Once you build a process with Nintex RPA, it's really not even an event anymore. This really helped us manage a bad situation."

Return on Innovation (ROI)

In this case, Nintex RPA was able to reissue cards at a rate of 6 per minute, and update and note 10 accounts per minute. By using Nintex RPA to automate this data breach recovery, this bank saved thousands of dollars in outsourcing. Cancelling and reissuing cards manually would have likely occupied valuable human resources for a weekend or more, delaying the process and risking human error. What's more, because fraudulent transactions were mitigated and customers were able to begin using their new cards quickly, any loss in interchange income was minimized. This bank was able to condense what would otherwise be a days-long process into a matter of hours. In doing so, they kept customers happy and reduced their exposure by notifying them of the changes quickly, updating their spending limits, and getting new cards into their hands fast.

"We would have had two choices. Our core does offer an outsourced solution where they would take care of the entire process for us, but we don't have control over it." stated the Assistant Vice President of Operations Systems. "The other solution is to dedicate several days to keying all of this in by hand…and I don't type that fast."

Ultimately, this bank made recovering from the Target data breach faster, easier, less expensive, and more accurate, by putting automated employees – not real ones – to work.

"When something like this happens, it's not going to happen once. So we built a process and scripts so we're prepared for the next one."

— Bank's Assistant Vice President of Operations Systems