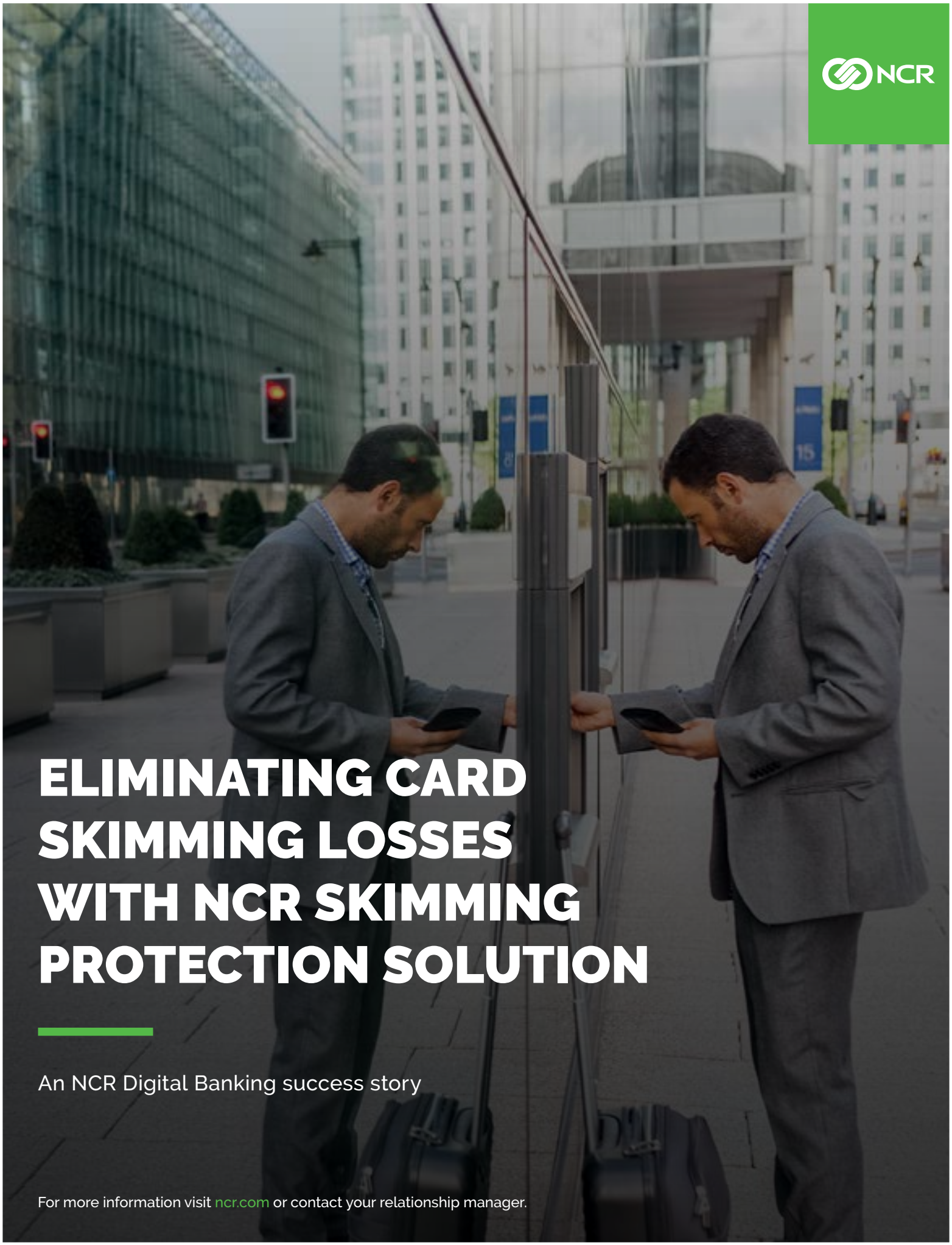


ELIMINATING CARD SKIMMING LOSSES WITH NCR SKIMMING PROTECTION SOLUTION

An NCR Digital Banking success story

For more information visit ncr.com or contact your relationship manager.

Key highlights

Industry/Market:
Retail Banking

Challenge:
The customer was experiencing high levels of false alerts from older versions of anti-skimming solutions. These alerts created additional workloads on the bank's fraud group to investigate if the attacks were legitimate.

Solution:
NCR Skimming Protection stops the ATM from operating when a criminal attempts to use a skimming device to record data from a card's magnetic stripe.

- The customer completely eliminated card skimming attacks on their ATMs
- The customer also saw a significant decrease in false alerts

> **The NCR team managed to deliver the complex solution on thousands of ATMs without any major problems and completed before the schedule.**
>
> — Senior Manager – ATM Hardware & Fraud, ATM Channel, NAMER FI

The challenge

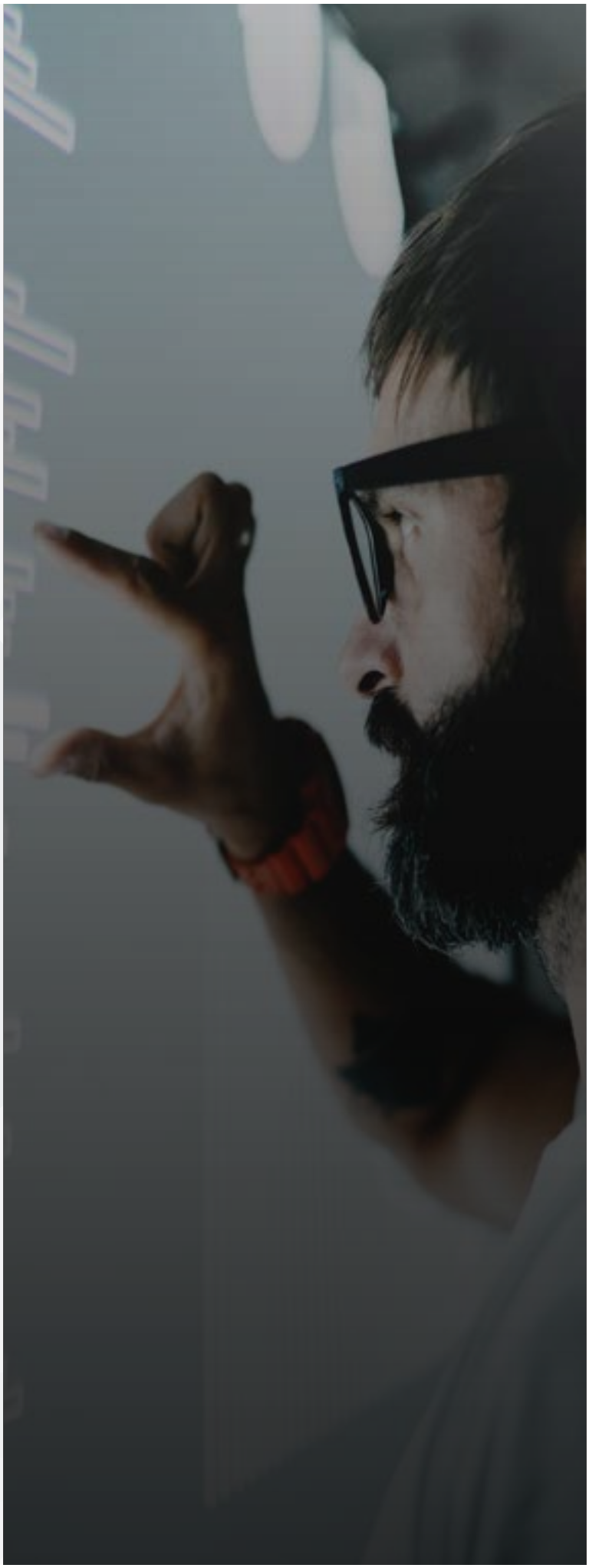
Between 2012 and 2014, an NCR banking customer had experienced one or two card skimming attacks every month, seeing $40,000 - %50,000 losses per incident--not to mention the negative impact to their brand and customer experience.

ATM skimming has quickly become more sophisticated due to organized crime. Skimming devices are getting smaller and more undetectable all the time. And with mobile phone technology, criminals are creating ATM PIN capture devices that can also send the image to a remote PC.

The problem continues to accelerate along with certain trends:

- The crime constantly evolves
- The criminals become ever more organized
- The crime ever more sophisticated
- Criminals migrate to the weakest link
- Skimming devices get smaller and harder to defeat

The impacts of ATM card skimming are significant, from lost consumer trust and negative brand experience to financial losses for the bank.



The solution

The customer chose NCR Skimming Protection Solution (SPS) to address their continuing situation with ATM skimming attacks. NCR Skimming Protection Solution is designed specifically for NCR ATMs and provides comprehensive protections through functionality to detect and jam most forms of bezel and insert skimmers. It provides additional anti-tampering sensors to protect the device from being disabled with sabotage and also provides physical protection components to prevent other forms of skimming attacks.

Detection and disruption technology

Detection is focused on the card data path, which minimizes the potential for false alerts. Integration with the ATM triggers both physical barriers to prevent cards from being inserted into the ATM. Customers can have the option to take the ATM out of service until the detected object is removed. (Note the customer in this case study did not choose this implementation option.)

Multiple sensors create a constantly changing, randomized stream of noise to disrupt and jam any devices that attempt to read the cardholder data. This means the criminal can't decipher the data when they remove the skimmer or recording device.

The customer was particularly impressed with the jamming technology and saw it as a key differentiator of NCR's solution versus competitor solutions.

Integrated diagnostics and state of health

Unlike third-party solutions, SPS has diagnostics and state of health indicators built in. This makes it easy for the deployer to monitor the device and take action when needed.

Future-ready solution architecture

SPS uses industry standard, expandable BUS architecture. New sensors and alarm devices can be added in the future to protect against new kinds of attack without having to replace the SPS module, making response time faster.

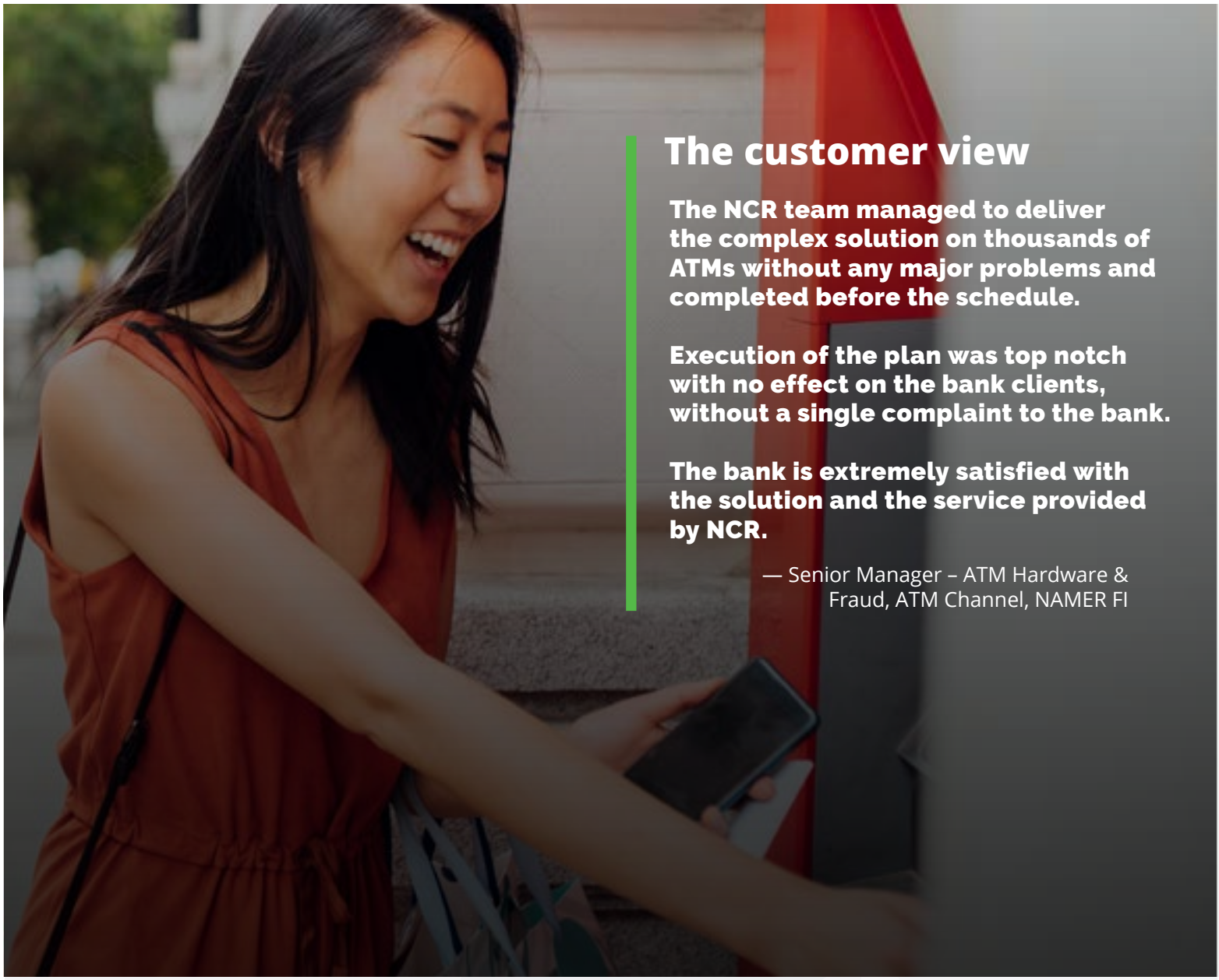
SPS uses Field Programmable Gateway Array (FPGA) architecture — so hardware can be repurposed via downloadable software.

Remote monitoring and superior manageability

Different software implementation scenarios are possible, depending on the target network environment. SPS will send status messages to XFS via the SUI Service Provider, and through SNMP. NCR Skimming Protection Solution can also operate in a standalone mode as well.

The solution benefits

NCR completed the deployment of SPS ahead of schedule, and the benefits were immediate--completely eliminating card skimming attacks in their ATM channel. As a result, all 4,600 of the bank's ATMs are now protected by NCR.



The customer view

The NCR team managed to deliver the complex solution on thousands of ATMs without any major problems and completed before the schedule.

Execution of the plan was top notch with no effect on the bank clients, without a single complaint to the bank.

The bank is extremely satisfied with the solution and the service provided by NCR.

— Senior Manager – ATM Hardware & Fraud, ATM Channel, NAMER FI

Why NCR?

NCR Corporation (NYSE: NCR) is a leading software and services-led enterprise provider in the financial, retail, hospitality, small business and telecom and technology industries. We run key aspects of our clients' business so they can focus on what they do best. NCR is headquartered in Atlanta, GA with 34,000 employees and solutions in 141 countries. NCR is a trademark of NCR Corporation in the United States and other countries.