Danske Bank Invests in Video Software for Fraud Detection and Anti-Money Laundering

Since Copenhagen-based Danske Bank began using March Networks® video surveillance systems in 2007, the risks facing the banking industry have changed dramatically. ➤

IN 2012, according to Thomas Johansen, director of the bank's Physical Security and Risk Group, Danske Bank had 36 robberies in Denmark alone. In 2018, as consumers performed more of their banking online and the number of branches decreased, there were only three bank robberies recorded. However, during the same time span, ATM crime increased dramatically — so much so that according to sources, the gross losses on Danish-issued credit cards amounted to more than $60 million US in 2018.

Today, the bank uses its video surveillance system as much to help combat fraud and money laundering as it does for physical security, said Johansen. The March Networks Searchlight™ for Banking software, in particular, has become an essential tool for protecting the bank's assets.

The Searchlight software, which integrates surveillance video with transaction data from Danske Bank's ATMs, alerts fraud investigators to transactions involving withdrawals just short of the daily threshold limit, and high-value withdrawals from newly activated accounts. Its daily reports include bank card numbers, which fraud investigators can use to identify cards that have been reported lost or stolen.

Approximately 500 Danske Bank employees have access to live and recorded March Networks video, including branch employees, fraud and anti-money laundering departments, ATM operations staff, security guards, health and safety personnel, and receptionists.

The reports also enable investigators to easily link to the recorded video to see the individual conducting the transaction. If the card owner is listed as a woman, for example, but a man is seen using the card in the video footage, it's a further indication that the transaction could be fraudulent. Investigators might then freeze the account, contact the bank card owner, and use the recorded video evidence to help build their case. ▶

The Searchlight software alerts [Danske Bank] fraud investigators to transactions involving withdrawals just short of the daily threshold limit, and high-value withdrawals from newly activated accounts.

In total, more than 50 Danske Bank operators use the software daily to detect and deter fraudulent activity. Danske Bank also plans to eventually use Searchlight to detect instances of money laundering, by configuring the software to report on a range of transactions indicative of suspicious behavior, such as high-value multiple deposits and transfers.

In the Nordic region, Danske Bank operates 102 retail banking branches in Denmark, 32 in Norway, and 35 in Sweden. In Denmark alone, it operates approximately 500 ATMs. Overall, the bank records video from approximately 4,000 cameras and has more than 500 March Networks video recorders, including 8732 Hybrid NVRs in its retail branches and head offices, and either 8704 or 8508 Hybrid NVRs in its ATMs.

In addition, Danske Bank has a presence in Kuala Lumpur, Germany, Poland, Latvia, Lithuania, India and the United Kingdom, where it provides banking services to Nordic companies or has technology centers and back office operations — all of which are also equipped with March Networks video surveillance systems. ➤
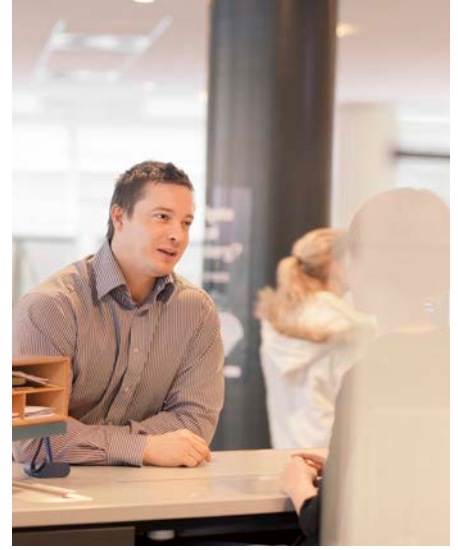
Johansen estimates that approximately 500 Danske Bank employees have access to live and recorded March Networks video. They include branch employees, fraud and anti-money laundering departments, ATM operations staff, security guards, health and safety personnel, and receptionists. Even kitchen staff and waiters use the system to monitor meeting rooms in the bank's head office in Copenhagen, so they know when to serve the next course and clear up following meetings.

To accommodate this broad access to video, system administrators use March Networks Command™ Enterprise Software to restrict access to cameras based on each employee's job description or department. This ensures that each user sees only the video they need to do their job, and meets key security and General Data Protection Regulation (GDPR) requirements for the bank.

As video surveillance proliferates across cities, law enforcement authorities make more and more use of the vast array of archived video captured by banks, retailers, schools and other organizations. No exception, Danske Bank is regularly asked to hand over video for police investigations involving robberies and other crimes, said Johansen.

During a terror attack close to one Danske Bank branch in 2015, for example, Johansen was personally involved in supplying police with video footage.

"Fortunately, in most cases, I can find the video needed in a few minutes and deliver it to police in a folder with the Command Client reviewer. That has really helped us out because three or four years ago, we would have to deliver the video on CDs or USB sticks, which was a lot more time consuming."

March Networks' Smart Search functionality enables users to quickly search for motion in a specific area of archived video by generating a list of all recorded events detected within that area. Additional March Networks search features — such as motion histograms, video indicators and visual finders — also help users zero in on the precise video evidence required.

Johansen is happy to help law enforcement with investigations, but hopes to come up with a solution that reduces the burden on Danske Bank personnel by giving police secure, limited access to video from select cameras during specific timeframes.

Currently, Danske Bank's alarm monitoring company has 24/7 access to the March Networks system and is able to pull up video from all branches remotely to verify the cause of an alarm activation. This makes it possible to dispatch police immediately if necessary, while avoiding false alarms.

The banking industry has changed dramatically since 2007 when Danske Bank first selected March Networks as its video surveillance partner. March Networks technology has also evolved, delivering ever-better performance as well as the video-based business intelligence capabilities customers like Danske Bank need to keep their assets secure. ◆

the **challenge**

Danske Bank, a Copenhagen-based financial institution with more than 200 branches in 10 countries, has seen a major change in the risks it faces as losses from ATM fraud have soared. It was clear that software able to detect suspicious transactions and capture clear video evidence could play an important role in helping the bank protect its assets.

the **solution**

Danske Bank expanded the capabilities of its March Networks video solution with Searchlight for Banking software. The intelligent software combines ATM transaction data with surveillance video in customizable reporting dashboards that highlight suspect transactions indicative of bank card theft or money laundering.

the **result**

Fraud investigators are now alerted to transactions involving suspicious deposits, withdrawals just below daily threshold limits, and high-value withdrawals from newly activated accounts. They can then use the data and Searchlight for Banking software to investigate further and provide evidence to law enforcement. The bank plans to expand its Searchlight capabilities by introducing video analytics, which will help detect instances of cash harvesting and money laundering.

MARCH®
n e t w o r k s