CARDTRONICS PERSPECTIVE

The billion-dollar security risk

How ATM operators can safeguard cash

Dan Antilley
Cardtronics

By Dan Antilley, Chief Information Security Officer, Cardtronics

How do you protect countless billions in cash hidden in plain sight around the globe? How do you keep it from the hands of sophisticated cyber crooks and organised adversaries galvanised by the prospect of such large sums?

Those questions keep security chiefs at the world's financial institutions and ATM operators awake at night because that cache of cash is held in over three million ATMs globally.

These concerns are especially critical as a growing number of banks and credit unions, eager to boost shrinking profit margins, look to ATM operators to manage their ATMs – both on- and off-premise.

I'm familiar with this angst after serving several years as director of Bank of America's global information security operations. I worked relentlessly with the best and brightest – both there and within the industry – to generate successful solutions that ensured the safety and security of our currency and customer information. In this endeavour, we constantly aimed to emulate and champion the best solutions and stay one step ahead of criminals.

Now, in my current role as the Chief Information Security Officer at Cardtronics – the sleepless nights continue. While I remain confident in our ability to keep the bad guys in check, we're never satisfied because they don't rest – so neither do we. That's why collaboration with all levels of law enforcement, fellow financial institutions and other security partners is essential. It proves a key differentiator throughout the lifecycle of threat management.

Real threats require real collaboration

As the world's largest ATM owner/operator, Cardtronics knows ATM security issues are increasingly complex. That's why in outsourcing ATM operations, financial institutions must ensure that operators are as vigilant as possible in protecting their cash, cardholders and brand reputation. In view of the growing sophistication and boldness of cyber crooks and gangs, a manager of ATMs can no longer do it alone the way many have done as recently as five years ago.

The threat of malicious attacks is constant and real. More than half of bank executives surveyed in 2017 said their ATM losses climbed in 2016 from 2015 – whether from computer fraud, malware or brazen crash-and-grab tactics. And bold they are, such as the Bonnie-and-Clyde-style Maryland couple who last year went on a three-state ATM theft spree, stealing cars, crashing them into convenience stores and dragging out cash machines with ropes or chains. Or there's the Houston, Texas gang whose ritual for prospective members has been to steal an ATM from hotels and elsewhere. On top of all that, ATM jackpotting, a technique which quite literally causes an ATM to spew forth all its cash, recently made its debut in the United States.

Looking to world-class fleet management

Today, when financial institutions are evaluating their security operations or considering outsourcing ATM fleet management to third parties, it's more vital than ever that they look for expertise in handling local and international ATM-related threats and incidents.

Well-prepared ATM fleet management today requires superior:

- **Internal security operations**, which coordinate all security-related departments and personnel, ranging from ATM engineers and repair staff to lawyers and risk managers. This ensures that everyone is on the same page security-wise, as well as understands their responsibilities and collaborates continually to stay on top of security developments.
- **Intelligence gathering and information sharing**, including retaining the services of national and international experts who specialise in and monitor cybercrime, skimming devices, physical theft and internal fraud. A world-class ATM operator would also share threats and related information with local and international law enforcement agencies. Doing so speeds the flow of information about ATM-related theft events and trends, and in turn allows ATM operators and law enforcement agencies to mitigate or even prevent damage and loss. The ATM operator should also be a collaborative participant in 'infosec' industry groups, such as the Financial Sector Information Sharing and Analysis Center (www.fsisac.com). The 7,000-member non-profit is considered the preeminent infosec group and focuses on analysis and information sharing to protect the global financial infrastructure against physical and cyber threats.
- **Forensic capabilities**, including an internal forensics unit with a toolkit to better understand the mindset of criminals and gain an upper hand against them.
- **Analytical skills** to examine and evaluate the intelligence and statistics gathered and shared with internal or external sources whether local, regional, national or global.
- **Crime-assisting tools** to help combat ATM-related thefts. For instance, in the UK – where physical theft of the entire ATM unit is common and thieves often delay opening it until confident they weren't followed – Cardtronics provides local police stations with GPS-tracking devices that are able to determine where stolen machines have been taken.
- **Proven skills for convincing fintechs to prioritise security issues.** These firms, which leverage ATMs as the nexus between the digital and physical payment environments, include those developing technology to perform digital-to-cash and cash-to-digital transactions. In the UK, Cardtronics and CashDash, a provider of multi-currency digital wallet technology, have integrated cardless cash withdrawal technology and foreign exchange functions at 5,000 of Cardtronics' Cashzone ATMs in London. In North America, FIS and Cardtronics continue on a path to integrate FIS Cardless Cash access across Cardtronics' ATM fleet in the USA.

The bad guys continue to become more sophisticated because the billions in cash lying in plain sight is a tempting target. As a result, the best ATM operators continually listen, learn, collaborate, evolve and improve in order to maintain world-class operations for combating this crime successfully. Their reputations – as well as those of the financial institutions and retailer brands they represent – depend on it. ■

In view of the growing sophistication and boldness of cyber crooks and gangs, a manager of ATMs can no longer do it alone

The best ATM operators continually listen, learn, collaborate, evolve and improve in order to maintain the strongest operations for combating ATM crime