# I AM THE NCR SKIMMING PROTECTION SOLUTION

## An NCR Secure™ Solution

## Fight back at ATM card skimming attacks

Protect your ATM network from the risk and associated costs of skimming protection attacks. Global losses from these types of attack exceed $2 billion annually. Don't become a statistic. Let NCR Skimming Protection Solution (SPS) help reduce the risk of attack while making sure your ATMs are always available to your customers when they need them.

### Protect cardholder data

NCR Skimming Protection Solution uses multiple jammers that generate multiple random signals, preventing any attempt by a criminal to isolate and record data from the magnetic stripe on the card. NCR SPS has a new design that focusses the jamming and protection on the actual card data path on the magnetic stripe. This means that even the smallest skimming devices won't be able to capture card data.

### SPS looks after itself

Unlike third party solutions, SPS has built-in diagnostics and state-of-health so that you can monitor the device and pinpoint whether it is functional or not; if it is not – action can be taken immediately.

### Enhance your protection with optional detection software

Real-time detection of the presence of a fraudulent device on the ATM means that you can manage your response to a potential attack before it even occurs. Settings can be configured to your unique environment and changes are managed by your application via APTRA™ XFS or by SNMP via your management system.

### Keep serving your customers

With NCR SPS's multi-layered approach to protection, there is no need to immediately take the ATM out of service if an attack is suspected. Even if a fraudulent device is detected, NCR SPS jamming remains in operation and cardholder data is protected. NCR SPS defends against attempts to tamper and disable the anti-skimming functionality by using sensors that can detect attempts to drill into the ATM fascia around the card reader area.

**NCR SelfServ™**

**PROTECTED**
READING DATA

**CONSUMER CONFIDENCE**

NCR

**Protect your investment while defending your ATMs from future attacks**
The threat from criminals continues to evolve. NCR understands that any anti-skimming solution should be quickly adaptable to exposure to new threats.

- NCR SPS has an industry standard expandable bus architecture that allows new sensors or alarm devises to be added in the future to protect from new forms of attack without having to replace the SPS module

- The architecture of SPS is fully configurable to meet your environment or adapted to meet the future threats as they emerge

- SPS is designed with programmable hardware using Field Programmable Gateway Array (FPGA) architecture and downloadable software

## Key features

### Anti-skimming protection

- Multiple random noise generators
- New design to focus the jamming at the potential point of compromise

### Detection and alerts

- For NCR SelfServ™ ATMs with motorized card readers detection is an option either at installation or at upgrade
- For SelfSev ATMs with DIP card readers, detection is available as the primary feature
- Can be integrated with APTRA XFS or SNMP

### Self-protection

- Integrated diagnostics and state-of-health monitoring

### Configurability

- Choose either the recommended settings or configure to address a unique environment or future threats

### Scalability

- Industry standard bus architecture allows for fast response to new threats and reduced development and certification cycles
- FPGA architecture – hardware can be repurposed via downloadable software

---