

## OPTEVA® BEZELSENTRY<sup>SM</sup> SERVICE

New service options add a critical layer to defending against card-skimming fraud

Every year, fraud caused by card skimming attacks costs financial institutions (FIs) and consumers billions of dollars, according to research by Aite Group. These attacks cause FIs to incur losses that extend far beyond the money stolen through fraudulent withdrawals, including substantial investments tied to reissuing compromised cards and loss of consumer confidence in the automated teller machine (ATM) channel. Findings by Javelin Strategy and Research suggest the fallout from skimming attacks may undermine consumer confidence in an institution itself, even, as 23 percent of victims who experience fraudulent ATM withdrawals will react by leaving their primary FI.

Mitigating the evolving threats can pose a challenge requiring multiple layers of protection. As part of its ATM Security Protection Suite, Diebold offers a comprehensive portfolio of skimming-protection solutions tailored to individual institution needs. Diebold has added an innovative, low-cost, threat-mitigation solution that offers an additional layer of security for Opteva terminals: the Opteva BezelSentry Service.

Available for Opteva terminals, the newly designed card reader bezel features geometric fascia alterations to help prevent skimming devices from reading a card's magnetic stripe and surface variations that will make it considerably more difficult for perpetrators to replicate and replace a bezel. A new mounting bracket feature allows a service

technician to quickly and easily change the bezel without having to remove the fascia, minimizing ATM downtime. Additionally, tamper-removal switch ensures that only a trained technician can change the bezel on an Opteva ATM. By design, the new bezel also serves to reduce false alarms at the ATM. Internal mounting features have been specially engineered to accommodate and enhance the effectiveness of Diebold's electronic skimming countmeasures which include the Advanced Skimming Detection and TMD Security solutions.

### Service Options

Three new bezel service offerings, an industry first, have been designed to meet the varying security needs of FIs. The service will allow FIs to have card reader bezels changed periodically, and even proactively, in an attempt to stay one step ahead of would-be perpetrators.

**DIEBOLD**

INNOVATION DELIVERED®

**Multi-Year/Emergency Bezel Replacement**

Offering the best value, the multi-year service plan is a contract that provides three scheduled bezel changes and the extra security of an emergency bezel option to be used anytime during the contract if the current bezel has been compromised.

*Highlights include:*

- Interchangeable bezel installed upon acceptance of program
- Scheduled bezel change at one-year program anniversary
- Scheduled bezel change at two-year program anniversary
- Emergency bezel option available upon customer request

**Annual Scheduled Bezel Replacement**

This service option is a contract offering that allows FIs to order a new bezel in between scheduled replacements if the current bezel has been compromised.

*Highlights include:*

- Current bezel replaced with interchangeable bezel upon acceptance of program
- New bezels installed annually

**Billed Work Bezel Replacement Offering**

This service option offers FIs the flexibility to replace bezels on an as-needed basis, without a contract.

*Highlights include:*

- Interchangeable bezels replaced as needed
- Interchangeable bezel can be installed across an ATM network or only on selected ATMs

In addition to implementing the interchangeable bezel, the following best practices will also help in mitigating skimming fraud:

- Build awareness among consumers, branch personnel and ATM service teams to help in the detection of devices added to an ATM's fascia. Visual cues such as tape residue near or on a card reader may indicate the former presence of a skimming device.
- Monitor the routine patterns of withdrawals and notify operators or FIs in the event of suspicious activity.
- Deploy video surveillance and monitoring systems to help effectively deter or detect placement of card skimmers and other fraudulent devices, such as PIN overlays and mini-cameras.
- Implement multiple layers of security to help deter and detect fraudulent attempts to provide the best approach to anti-skimming.

To learn more about Diebold's multi-layered security solutions, contact [productinfo@diebold.com](mailto:productinfo@diebold.com) or call 800.999.3600.

**Contact Information:**

Diebold, Incorporated  
Post Office Box 3077  
Dept. 9-B-16  
North Canton, Ohio 44720-8077

800.999.3600 USA  
330.490.4000 International  
email: [productinfo@diebold.com](mailto:productinfo@diebold.com)  
[www.diebold.com](http://www.diebold.com)

© Diebold, Incorporated, 2011.  
File No. 98-181.

**DIEBOLD**

INNOVATION DELIVERED®