

Which Anti-Skimming Model Best Protects Your Customers?

ACG Enhanced Card Security (ECS®) Products

	ECS Basic	Communication Module Paired with ECS Basic	ECS Dual	ECS Detect	ECS 4-in-1
DIP Compatible				•	•
Motorized Compatible	•	•	•		
Sensor Technology				•	•
Jamming Technology	•		•		•
Communication		•	•	•	•
Monitoring <small>Send real-time data to monitoring center</small>			•	•	•
Data Logger <small>Saves data internally for transfer to center</small>			•	•	•
LCD Display			•	•	•
Dimensions	25x110x75 mm	25x104x70 mm	37x145x85 mm	37x145x85 mm	37x145x85 mm
Power	24 V DC	5 V DC	24 V DC	24 V DC	24 V DC
Memory	N/A	N/A	4 GB	4 GB	4 GB



INTRODUCING THE

ECS4-in-1



About ACG

Since 1986, ACG has been an industry leader in providing comprehensive business solutions to financial institutions and service providers across the globe. ACG's diverse product portfolio includes ATM refurbishment, spare part solutions, repair, managed services, compliance solutions, regional field service, and more! With three global offices, you can count on ACG to meet your logistical requirements, all while providing the perfect combination of expertise and knowledge.

Global Headquarters

5010 McGinnis Ferry Road, Alpharetta, GA 30005
800.536.5085 • sales@ACGWorld.com

ACGWORLD.COM

A Single Solution.
Multi-Layered
Skimming Protection.



Professional Anti-Skimming Solutions



ECS4-in-1

How ECS 4-in-1 Detect Works

ECS 4-in-1 is truly a unique anti-skimming solution for dip card readers, as it offers a combination of detection and jamming protection. ECS 4-in-1 protects ATM users against skimming attacks through sensing technology. It also provides a shield of skimming protection by creating random, disturbing frequencies that scramble skimmers (jamming). Therefore, ECS 4-in-1 can detect the physical installation of skimming devices while simultaneously deactivating them. Additionally, ECS 4-in-1 includes monitoring, communication and data logging functionalities.



What is Skimming?

Skimming devices are those that illegally record personal identification and financial information from the magnetic stripe of credit and debit cards. These devices include skimmer card readers and even hidden ATM cameras!

- They generate \$1 trillion cash transactions annually.**
- \$500,000,000 of this cash is obtained fraudulently by ATM Skimmers every year!**

**There are more than
400,000 ATMs in the U.S.***

Why both Detect and Jamming Technology are Essential

Anti-skimming devices that solely use sensing technology can detect skimmers; however, they cannot completely prevent fraudsters from being able to obtain confidential credit and debit card information. Reason being, deactivating the card reader on an ATM does not necessarily deactivate the skimming device, as most skimming devices have power sources independent of the ATMs on which they are hosted.

Let's say a fraudster installs a skimming device

on an ATM that is armed with a detection-only anti-skimming module. The module will send an alert when the skimmer is detected and in some cases shut down the card reader to prevent ATM use. Despite these precautions, however, the skimming device will remain powered and the ATM will still appear to be fully functional to ATM users. Therefore, in the time that it takes the service provider to respond to the skimming alert, card information can still be compromised if a patron attempts to use the ATM. For this reason, a second layer of jamming protection is needed to comprehensively prevent skimming attacks.

*Wired Magazine: http://www.wired.com/culture/culturereviews/magazine/17-09/st_atms

**Today Show Broadcast: <http://today.msnbc.msn.com/id/26184891/vp/37775288#37775288>