

# REDEFINE YOUR EDGE.

DIEBOLD ACTIVEEDGE™ PROVIDES  
GAME-CHANGING ATM SECURITY.



**DIEBOLD**®

# PROTECT YOUR INVESTMENT, FLEET AND CONSUMER.

THE THREAT OF SKIMMING IS REAL AND MUST BE ADDRESSED.

Today's consumers are relying more and more on the self-service channel. They expect service that is fast, efficient and, most importantly, secure. But, just how secure is the ATM experience? And, what exactly does a breach in security cost?

Each year 1.7 million ATM locations host 40 billion cash withdrawals across the globe<sup>1</sup>. This translates to 40 billion opportunities for criminals to take advantage of financial institutions and their customers. And, with skimming accounting for 98 percent of total ATM card fraud loss<sup>2</sup>, it is **the most significant threat at the terminal**. The average skim costs \$50,000 in damages<sup>3</sup>, making the financial impact clear. Damaged consumer confidence is harder to calculate but arguably even more important to consider.

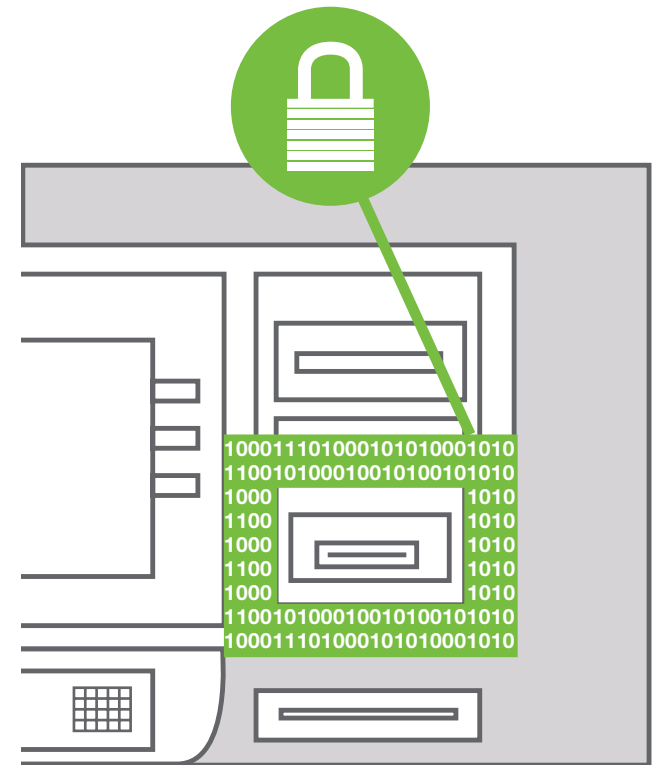
## ATM SKIMMING RESULTS IN AN ESTIMATED \$8.5 BILLION IN LOSSES ANNUALLY.<sup>4</sup>

<sup>1</sup> Source: "ATM Skimming Costs Banks Money And Reputation," Tyco Integrated Security, 2014

<sup>2</sup> Source: European ATM Crime Report, 2014

<sup>3</sup> Source: "Credit Card And ATM 'Skimming' Is Big Business," Here & Now, 2014

<sup>4</sup> Source: "ATM Skimming Costs Banks Money And Reputation," Tyco Integrated Security, 2014



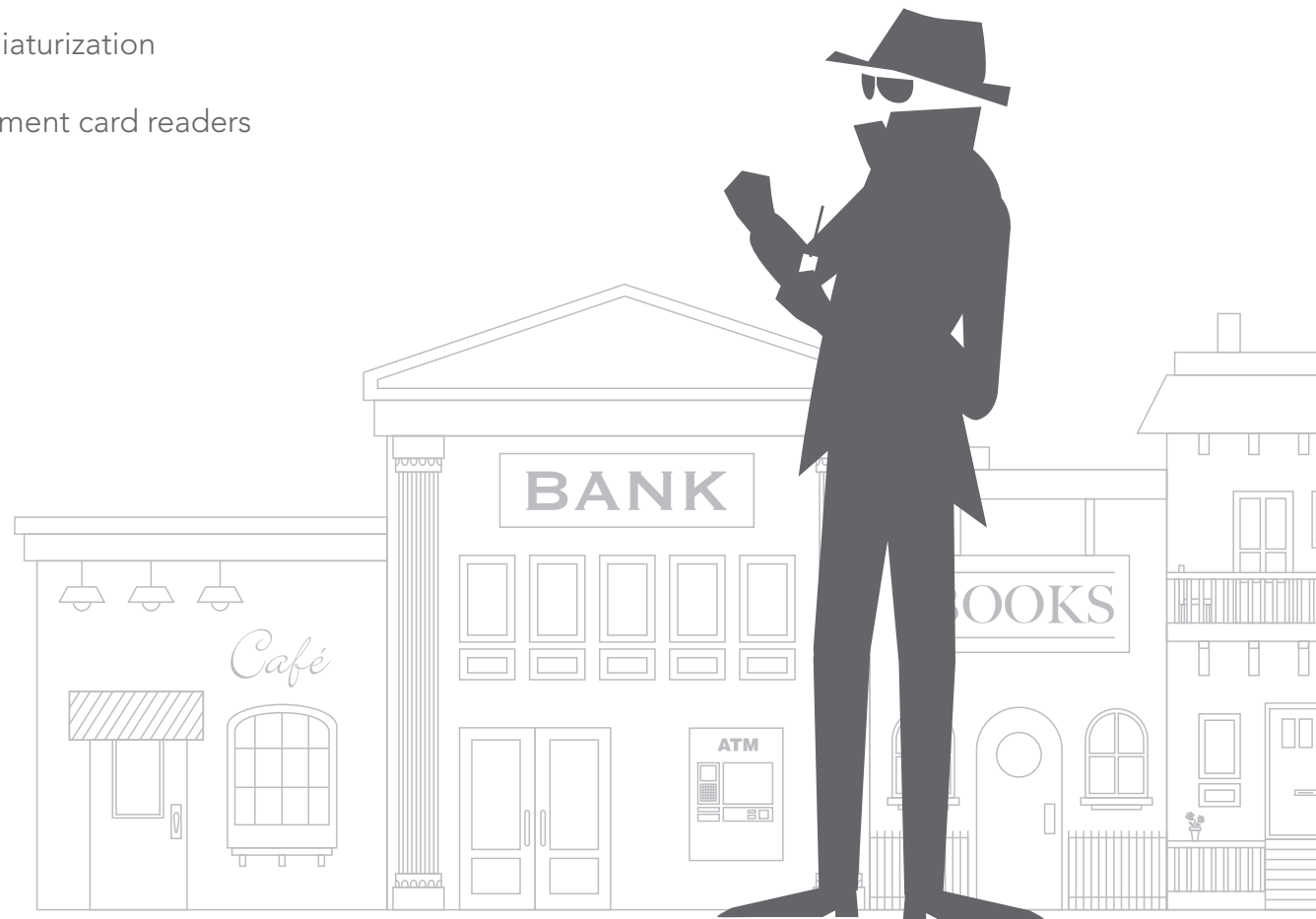
**PROTECT AGAINST  
SKIMMING**

# INVEST IN SOLUTION TECHNOLOGY.

BECAUSE CRIMINALS ARE INVESTING IN TECHNOLOGY, TOO.

Recent advancements in skimming technology have made skimming devices harder for financial institutions to detect and easier for criminals to locate and purchase. **Skimming enhancements include:**

- Battery improvements and component miniaturization
- Internal and combined attacks and replacement card readers
- Smaller, slimmer designs
- Ability to mitigate jamming technology



# THE EVOLUTION OF SKIMMING



**2002 – 2007**

**Criminals attach a skimming device to the card reader** in order to capture consumer information and download it onto a laptop.




**2008**

**A micro spy camera** is added to capture PIN-entry codes.




**2009**

**New devices** that consist merely of a battery, flash memory card and mini USB port make skimmers harder to detect. Micro spy cameras become smaller and more difficult to find.



**2010**

**Criminals replace micro spy cameras with PIN-pad overlays** that record PIN-entry keystrokes, enabling stolen data to be packaged and sent to the criminal's mobile phone.



**2012**

**Design improvements make skimmers paper thin.** Skimming production becomes widespread, and criminals can easily purchase professional skimming devices online.



**2014**

**A new type of skimming device is discovered** that is inserted into the motorized card reader and bypasses existing low-and mid-tier anti-skimming technologies.



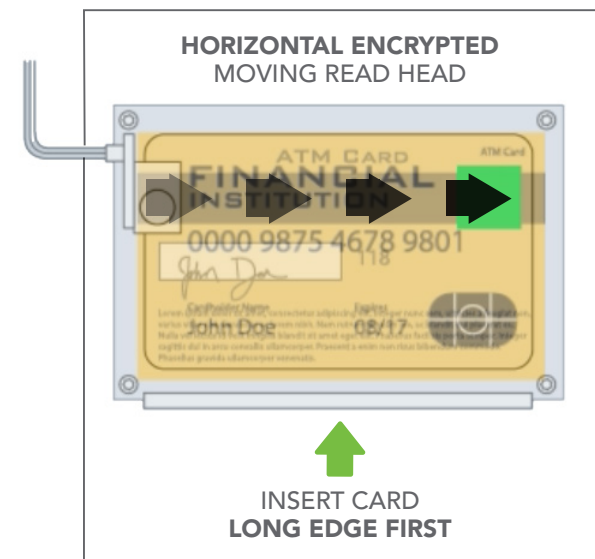
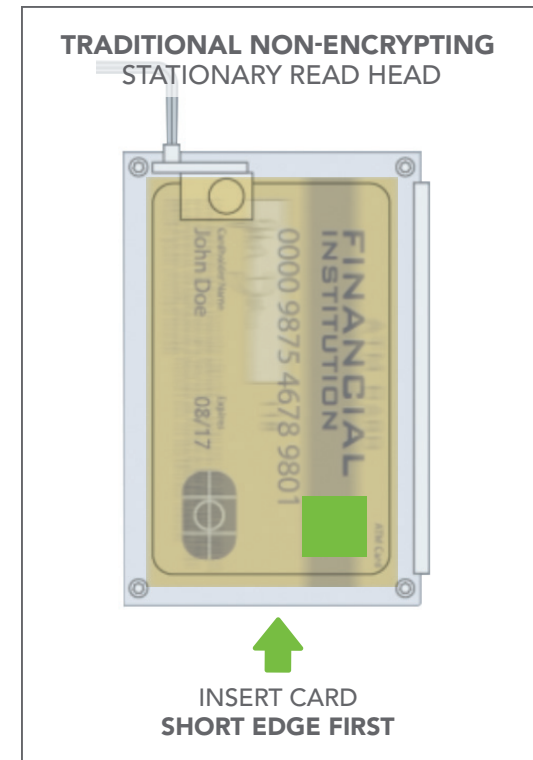
# TURN ATM SECURITY ON ITS SIDE. LITERALLY.

PAIR LONG-EDGE INSERTION WITH AN ENCRYPTED MOVING READ HEAD FOR COMPLETE COVERAGE.

A breakthrough in ATM security, Diebold ActivEdge™ counteracts skimming by altering the way an ATM card is inserted and read. Current skimming technology relies on the ability to read an ATM card's entire magnetic stripe in a short-edge orientation. ActivEdge requires consumers to insert their cards long edge first, **making it impossible to capture the card's information with today's skimming technology.**

Additionally, ActivEdge is the world's first card reader to utilize an encrypted moving read head. This **eliminates a fundamental weakness** that all of today's skimming devices attack, preventing criminals from reading the card's magnetic-stripe information.

## DEFEAT EVERY KNOWN TYPE OF SKIMMER ON THE MARKET TODAY.



# EXPERIENCE A COMPREHENSIVE SOLUTION.

ACTIVEDGE IS MORE THAN JUST A SKIMMING DEFENSE.

Designed to prevent physical, informational/logical and card-related attacks, ActivEdge is the most comprehensive card-reader solution on the market. It features:



**Encrypted communication** – Eliminates USB sniffing and the ability to capture and track card data by ensuring secure communication from the read head to the processor.



**Paired devices** – Prevents the installation of fraudulent devices with software that pairs each ActivEdge card reader with a specific terminal.



**Automatic gate-locking functionality** – Enhances security by counteracting card trapping and phishing.

# EXPERIENCE A COMPREHENSIVE SOLUTION.

ACTIVEDGE IS MORE THAN JUST A SKIMMING DEFENSE.

100101  
000010

**Advanced skimming detection (ASD)** – Utilizes a highly sophisticated algorithm to discriminate between skimmers, environmental factors and cardholder activity.

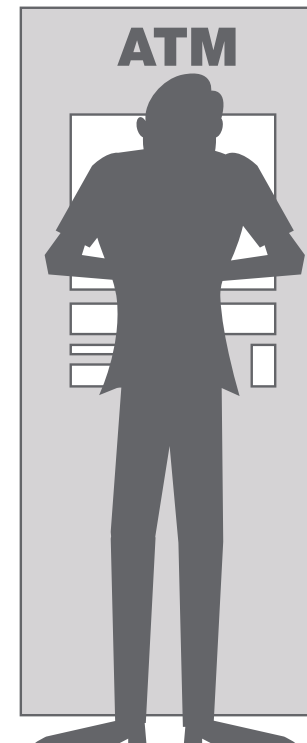


**Advanced skimming prevention (ASP)** – Detects skimming devices, directs alerts and closes the shutter on a motorized card reader within 15 seconds of detection.



**EMV Level 1 certification** – Meets EMV compliance deadlines for a smooth transition.

Diebold has made ActivEdge available to all OEMs. As a leading-edge security provider, Diebold offers the industry's most innovative secure card reader to all ATM OEMs through the ActivEdge Reseller's Agreement.



# EXPECT MORE FROM A HIGH-END OFFERING.

LOW- AND MID-TIER SOLUTIONS LEAVE YOU EXPOSED.

As a comprehensive solution with advanced functionality, ActivEdge is superior to low- and mid-tier fixes. It prevents the same attacks, but **also provides advanced protection against:**

- Internal skimming
- USB sniffing
- Device substitution
- Card trapping

ActivEdge is the only solution on the market that offers an encrypted moving read-head, encrypted communication between the card reader and ATM processor, and long-edge card insertion to limit criminal access to magnetic-stripe data. It also delivers reliable trapping and phishing protection.

Solutions such as jamming can be sensitive to false alerts, putting a terminal out of service until the issue is resolved. As an entire card reader, ActivEdge is also an integrated solution compared to low-and mid-tier anti-skimming devices that require additional hardware components and pose a greater security liability.





# REALIZE DRAMATIC SAVINGS.

INVESTING IN THE RIGHT TECHNOLOGY REDUCES OVERALL COSTS.

With skimming as the most prevalent ATM crime, and trapping and phishing incidents nearly doubling in 2013<sup>5</sup>, financial institutions can't afford not to be proactive. What's more, they must consider the incalculable cost of brand damage and customer churn that skimming attacks cause.

Additionally, ActivEdge improves total cost of ownership (TCO). With a longer lifespan and greater reliability than traditional card readers, it supports 1.3 million transactions versus 600,000 from a traditional card reader. Significant design improvements enable ActivEdge to offer as much as 27 percent more uptime. ActivEdge is EMV compliant and water resistant and is equipped with reporting functionality to deliver troubleshooting, service diagnostics, forensic data and log files.

<sup>5</sup> Source: EAST Report, 2013

<sup>6</sup> Source: "Credit Card And ATM 'Skimming' Is Big Business," Here & Now, 2014

<sup>7</sup> Source: Yearly Impact Value Calculator, Diebold, 2014

<sup>8</sup> Source: Yearly Impact Value Calculator, Diebold, 2014

## WHAT YOU'RE SPENDING ON CARD FRAUD

THE AVERAGE SKIM =

**\$50,000**<sup>6</sup>



CARD TRAPPING =

**\$1,000**<sup>7</sup>

PER INCIDENT



JUST **10 SKIMS** AND **20 TRAPPING** INCIDENTS

A YEAR =

**\$520,000**<sup>8</sup>

IN LOSSES



# PROVIDE A CONSUMER-FRIENDLY EXPERIENCE.

## RESEARCH INDICATES CONSUMERS READILY ACCEPT ACTIVEEDGE.

Diebold conducted focus groups around the world. These studies showed that **consumers readily accepted the slight behavior change** required by ActivEdge. Globally, 79 percent of users responded positively to long-edge card insertion without any prior knowledge of its added security benefits. Once informed, 92 percent scored it toward their most desired experience?

In addition, ActivEdge is equipped with red and green indicator lights that signify whether or not the card has been correctly inserted. Blink rate and LED control further enhance consumer experience.



# EIGHT OUT OF 10 USERS

**CORRECTLY INSERTED THEIR  
CARDS WITHOUT GUIDANCE.<sup>10</sup>**

<sup>9</sup> Source: LECR (Long-Edge Card Reader) Summary, Lextant, 2012

<sup>10</sup> Source: ActivEdge Card Reader Survey, Diebold, 2012

# TAKE A PROACTIVE APPROACH.

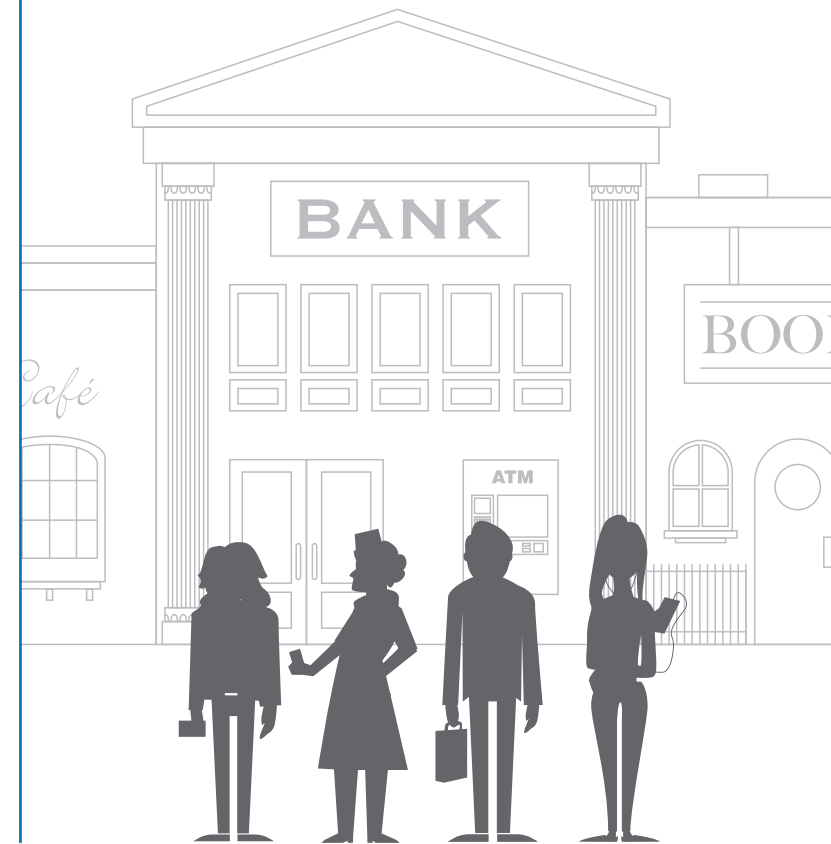
## WAITING FOR EMV ADOPTION IS A RISK NOT WORTH TAKING.

The EMV shift is a hybrid approach, and consumers will have cards with both chip and magnetic-stripe functionality for several years at least. In fact, Europe has been using chip cards since the 1990s and still issues cards with magnetic stripes. As long as the stripe is present, the card is vulnerable to skimming. Until global adoption of EMV occurs, most financial institutions also will accommodate foreign transactions without chip in order to sustain their surcharge fees, and they will have a continued need to counter this risk.

## DON'T BE LEFT BEHIND.

As criminals continue to develop new ways to capture data, it is critical that financial institutions take skimming threats seriously. Invest in a forward-thinking solution, or expect consumers to seek financial institutions that are willing to adapt. [Contact a Diebold representative today.](#)

TO LEARN MORE, VISIT  
[WWW.DIEBOLD.COM](http://WWW.DIEBOLD.COM)  
OR CALL **800.999.3600**





We've got a solve for that.™

© Copyright 2015 Diebold, Incorporated. All rights reserved.