ATM Industry Statement on Black Hat Briefing

For immediate Release, July 2010

Sioux Falls, SD, USA - The ATM Industry Association (ATMIA) (www.atmia.com), a global non-profit trade association with over 1750 members in 50 countries, today expressed its confidence in the industry's software and other critical systems, which are subject to robust governance, standards and industry best practices. The association reaffirmed this standpoint after a recent demonstration by ethical hacker and security professional Barnaby Jack, which indicated that certain ATMs can be "jackpotted".

At a Black Hat briefing[1] in Las Vegas this week, Jack, who is director of security research for IOActive™, gave an ATM security demonstration entitled "Jackpotting Automated Teller Machines Redux." His briefing focused on apparent vulnerabilities in ATM security and whether they can be exploited via local and remote attacks. He outlined a multi-platform ATM rootkit – a type of software that can be deployed, once a hacker or "insider" has gained unauthorized access to the system, to allow them to maintain administrative privileges to the system without being detected.

[1] Black Hat Briefings are leading industry events aimed at sharing practical insights and timely, actionable knowledge about logical security. Ethical hacking is a common practice in which experts attack a technology or network in a controlled environment to identify vulnerabilities a malicious hacker could potentially leverage. The goal is to deliver the intelligence needed to enable the mitigation of potential threats. Black Hat presenters typically notify manufacturers of their findings 90 days in advance of their demonstrations, providing affected companies with the opportunity to remediate issues before briefings are conducted. It is a responsible approach intended to benefit the entire financial services industry.

"This type of research conducted by professionals like Jack should be leveraged by our industry to improve ATM security, " said Mike Lee, CEO of ATMIA. "Even though we have produced a whole set of ATM lifecycle security best practices, including ATM software governance guidelines, we are always looking to raise awareness to continuously improve the security of the ATM channel in a global software environment that is faced with an evolving risk of fraud."

Independent Black Hat security briefings remind industry practitioners to stay vigilant, especially in regard to new and emerging threats. And leading ATM vendors have urged financial institutions to proactively manage the security of their ATM networks. While ATM manufacturers have targeted substantial investments in the development of security solutions to make sure that the ATM's IT systems are fully protected, it is necessary for ATM deployers to implement all relevant security initiatives to effectively combat fraud and cybercrime.

"ATM security is one of the most technically challenging areas of a financial institution's operation," Lee stated. "To ensure the most effective protection against a variety of threats – including internal, external, physical and logical threats – the industry advises financial institutions to implement and maintain a comprehensive, multi-layered security approach. In addition, ATM security programs should be regularly monitored, reviewed and updated to anticipate and mitigate changing threats."

The criminal industry is constantly changing its business models to gain the maximum "Return on Investment". Brian Nagel, Assistant Director, U.S. Secret Service, has recently stated: "Cybercrime has evolved significantly over the last two years, from dumpster diving and credit card skimming into a full-fledged online bazaar full of stolen personal and financial information."[2]

Multiple regulations, standards and best practices for ATM security include the Payment Card Industry (PCI) global security requirements (such as PCI DSS and PCI PA-DSS), ATMIA's set of international best practices, Ansi X9, the European Central Banks' ATM Best Practices Guides as well as guidelines and rules set by ATM networks and regulatory authorities across the world.

[2] Extract from the "DATA BREACHES: WHAT THE UNDERGROUND WORLD OF "CARDING" REVEALS", Kimberly Kiefer Peretti,U.S. Department of Justice.

“Along with our vendors, we take on board recommendations from consultants such as Barnaby Jack and remind all our members to revisit the wealth of security information, standards and recommendations already available to protect the ATM’s trusted environment,” Lee added. “We need to maintain a total approach to security in order to retain the trust that consumers have put in self-service.”

-Ends -

ABOUT ATMIA (www.atmia.com)

The ATM Industry Association is a global non-profit trade association with over 1,750 members in 50 countries. Its mission is to promote ATM convenience, growth and usage worldwide, protect the ATM industry’s assets, interests, good name and public trust; and provide education, best practices, political voice and networking opportunities for member organizations. In June 2003, ATMIA established the Global ATM Security Alliance (GASA) with the mission to employ global security resources in a united alliance in order to protect the ATM industry from criminal activity.