

**FOR IMMEDIATE RELEASE (May 22, 2006)**

**CONTACT: Jim Milford or D.C. Page, (305) 373-8488**

**[jmilford@verasysllc.com](mailto:jmilford@verasysllc.com) or [dcpage@verasysllc.com](mailto:dcpage@verasysllc.com)**

## **Miami Company Foils Identity Thieves**

**Miami, Florida** –Every time there's another front page story about the theft of customer personal identity information from a corporation, the phones start to ring at Verasys, LLC.

Each corporate crisis is a new business opportunity for the Miami-based company, which is in the business of risk mitigation services and has developed a worldwide reputation for plugging the holes in a company's security programs.

“It's a nightmare when a corporation, university, bank or government has to admit that its security has been breached and the personal information of thousands and perhaps millions of people -- such as their full name, Social Security number, date of birth, account number, email address, mailing address and telephone number -- is now out there, waiting for someone to steal their identities,” said Russ Owens, Senior Managing Director and Southeast Regional Director, who manages the accounts of the company's Fortune 500 clients. Owens is the former Director of Security, Worldwide Sales and Services, IBM and Executive Director of the Atlanta Crime Commission, with extensive worldwide experience in physical, information and data security.

“Verasys has brought together a number of people with vast experience in the security field and we have developed a proprietary protocol aimed at rapidly

assessing a company's security issues, said D.C. Page, the company's managing partner.

"Our protocol mirrors a multinational corporation's structure so it tracks personal identity information from the moment it is collected through all the steps of processing," he said.

Page is a former U.S. Customs Agent who, in his previous positions as Senior Managing Director of Kroll Associates and IPSA International's Miami office, worked on such projects as the Dale Earnhardt death investigation for NASCAR and the 2000 Presidential Election Florida recount.

"It's a three-phase system," said Owens. "We look at physical security and how personal identifying information is being protected as it flows through business processes from both an IT and non-IT (soft-copy) perspective," he said. For example, he said, a company often will put enormous energy into protecting information in the technology environment, making sure data is absolutely secure from outside hacking. But these same companies may fail to protect personal identity information in other formats, perhaps leaving PII information on work stations or boxes of credit card receipts in unsecured areas. "You can't just buy software and think you are protected," he said.

"Many times lower paid service employees, contractors, and vendors, have total access to offices and secure areas day and night," he said. "Nobody notices them as they move about. It's easy for them to steal information, and there are people out there who search them out and offer large sums of money for them to do so."

Owens added, "we seen some cases where in fact professional thieves get themselves hired into a particular company just to steal proprietary information."

But, Owens said, the answer is not just locking everything down. “It isn’t that simple,” he said. “The data must be secured but still be available for its intended purpose.”

He said, “The youthful hacker of yesterday has been replaced by well-educated and trained individuals that are part of organized crime groups that are primarily resident outside the United States. These groups have one objective in mind: identify companies with personal identity information and penetrate their facilities and business processes by any means possible, in order to obtain personal identity information that can be sold on the black market and the underground world of criminals.”

In the post 9/11 era, the Federal Trade Commission has been more aggressive, conducting similar audits of its own and acting much like government bank regulators, added Page. “When we identify a problem, the company has a chance to correct it proactively. But when the FTC gets there first, the problem may become very public and have significant penalties attached.”

Verasys’ proprietary personal identity information protection program is called VPII<sup>SM</sup>. The process can safeguard personal identity information from those who would use it for criminal purposes and ensure compliance with FTC, FCRA, HIPPA, GLB and related regulatory and industry guidelines.

Verasys is headquartered in Miami, with offices in Atlanta, Dallas and Buenos Aires, and has affiliate offices throughout North America, Latin America and Europe. Specializing in gathering and analyzing information, Verasys provides a wide range of international risk mitigation consulting services including litigation

support, asset searches, financial and computer forensics, due diligence, security assessments and crisis management.

Verasys maintains an international network of high-level professionals experienced in investigation, financial and computer forensics, security, international and local law enforcement, banking and law. They gather and analyze information to enable businesses to minimize their risks by providing market intelligence, screening potential alliances, establishing security processes, investigating fraud, handling workplace violence, providing expert witness services and more.

To learn more about VPII<sup>SM</sup> personal information protection system and Verasys LLC, please visit [www.verasysllc.com](http://www.verasysllc.com) or call 305-373-8488.