



NEW RULES, LEADERSHIP WILL ATTEMPT TO ADDRESS EVOLVING GLOBAL THREAT, ACCORDING TO IDENTITY THEFT ASSISTANCE CENTER 2010 OUTLOOK

WASHINGTON, DC, December 10, 2009 – [ITAC, the Identity Theft Assistance Center](#), has released the ITAC Identity Theft Outlook for 2010 based on developments over the past year and what’s ahead in 2010, including trends in criminal activity and law enforcement, impact of the “Red Flag” rules for identity theft and the Administration’s cybersecurity policy.

“We are seeing positive developments on the federal and state level, including the aggressive prosecution of identity theft criminals. However, identity crime, especially Internet-based crime by organized criminal groups and individual criminals, continues to menace consumers and the economy,” said ITAC President Anne Wallace.

The following are six trends ITAC anticipates in 2010:

- 1. An emerging breed of cyber bank robber.** The use of official-looking emails to acquire personal information, called phishing, is a familiar threat. But security experts have identified a disturbing new twist – criminals use malware to steal usernames and passwords and recruit accomplices as “money mules” to open phony accounts and transfer funds. “The convenience of technology is bittersweet, bringing with it immediate gratification from shopping online to chatting with friends. With convenience comes greater security risks as more sophisticated fraudsters take advantage of consumer and business vulnerabilities,” said Michael Stanfield, CEO, [Intersections Inc.](#) “It is the responsibility of consumers and businesses alike to demand the best security protection and to implement it into their everyday experiences,” he said.
- 2. Fewer silos and more collaboration on cyber security.** The Obama administration will continue to break down silos within the government and collaborate more with industry as they develop and implement cyber security policy. The administration is expected to announce the appointment of a cyber security czar whose job will entail orchestrating and integrating all cyber security policies for the government.
- 3. Expanded use of identity management solutions to address identity theft, data breaches, and cyber crime.** Digital identities are still less secure than physical ones, but progress is being made toward understanding how to integrate the disparate elements of identity in the digital age. The use of identity management solutions to combat identity theft, data breaches and cyber crime is essential but difficult to implement ubiquitously. [“The Center for Applied Identity](#)

[Management](#) is creating a knowledge base to provide researchers, practitioners, and policy makers with an integrated data set of threats, solutions, and needed capabilities. The analysis of this information will lead to applied research projects that will provide new and innovative solutions to challenges created by a growing digital world,” according to Executive Director Gary R. Gordon.

4. **A bumpy start for “Red Flag” rules.** The Fair and Accurate Credit Transactions Act (FACT Act) requires all businesses and organizations that handle sensitive consumer data to establish an Identity Theft Prevention Program that detects activity that could indicate identity theft. The Federal Trade Commission (FTC) has delayed enforcement of the rules until June 2010 to give companies time to prepare. The American Bar Association and the American Institute of Certified Public Accountants are taking legal actions to exempt lawyers and CPAs from the rules. Consumers will face questions about address changes and other behavior – such as missed payments, changes in spending patterns and cellular call patterns – from more businesses than ever before. The changes could be met with annoyance until customers become accustomed to new levels of scrutiny.
5. **Stiffer sentences for identity theft.** Courts are imposing stiffer sentences on identity theft criminals. The law requires a mandatory two-year sentence for aggravated identity theft. Prosecutors are pursuing additional jail time for related felonies, such as wire fraud and use of unauthorized access devices (credit cards). In late 2008, the leader of an identity theft ring in Southern California was convicted on 60 identity theft- related charges and sentenced to more than 20 years in prison.
6. **Possible federal regulation of breaches of consumer data.** Two Senate measures that would regulate how both public and private sector organizations protect personal information have cleared the Senate Judiciary Committee, and have been placed on the calendar for consideration by the full Senate. The full impact of any federal legislation will depend on whether the measures would preempt existing state laws.

About ITAC

ITAC, the Identity Theft Assistance Center, is a nonprofit coalition of financial services companies that display the ITAC logo to demonstrate their commitment to protecting customers from identity theft. ITAC’s victim assistance service – which has helped more than 60,000 consumers recover from identity theft – is available at no cost to the millions of consumers who have an account at an ITAC member company. Through its partner Intersections Inc., ITAC offers the ITAC Sentinel® identity management service (www.itacsentinel.com).

###

Contact :
 Kate Ennis
 (301) 580-6726
kate@enniscommunications.com