

# Solutions

## AaSys Introduces Two New Valuable Services!

### 2008 SECURITY INITIATIVE: LANSEC IMPLEMENTATION

The irony of the current lack of deployment of internal safeguards is that the majority of system's crimes are launched internally – either by bank employees or other individuals gaining unauthorized access to systems. To harden internal security, AaSys introduces the 2008 Security Initiative: LANSEC Implementation.

This security initiative is based upon the following methodology, which includes:



1. **Securing USB drives and CD/DVD drives on desktops** - deploying GFI's EndPoint Security to prevent data leakage by allowing an organization to easily control desktop devices. In addition, each MAC (Workstation Network Card unique physical address) will be aligned with the connecting port on the switch.
2. **Introduce Microsoft IPsec encryption on local LAN traffic** - All data flowing between computers will be encrypted.
3. **Configuring managed switches to allow for Port Security** - The security on managed switches will be hardened by attaching a specific network device to a corresponding port on the network switch. With implementation of this security measure, an unauthorized network device that is plugged into a wall jack will no longer be given network access.
4. **Deploying Service Pack 3 for Windows XP** – this offers a more robust remote desk top client and new security features.
5. **Hide folder shares from unauthorized access** - AaSys will configure and implement Access Based Enumeration, a file share structure whereby users not authorized to access specific folders will not have the ability to see those file shares in the folder tree.

*Ensure that internal network access is as safe and secure as your external security stance. Engage AaSys' LANSEC Initiative 2008!*

### RED FLAGS RISK ASSESSMENT – IDENTITY THEFT PROGRAM

The FACT Act (Fair and Accurate Credit Transactions Act of 2003) establishes a deadline of November 1, 2008 for creditors to implement a written Identity Theft Prevention Program. Under this new rule, which was established by federal banking regulatory agencies and took effect January 1, 2008, each financial institution's Identity Theft Prevention Program must include: reasonable policies and procedures for detecting, preventing and mitigating identity theft and enable the financial institution to identify relevant patterns, practices, and specific forms of activity that are 'red flags' signaling possible identity theft and incorporate those red flags into the institution's program.

AaSys' Identify Theft Program Risk Assessment is designed to ensure that community banks meet these regulatory expectations and to provide guidance in bringing plans into compliance.

The following types of Red Flags activities will be evaluated:

- 🚩 Alerts, notifications or warnings from a Consumer Reporting Agency
- 🚩 Suspicious documents
- 🚩 Suspicious personal identifying information
- 🚩 Unusual use of, or other suspicious activity related to a covered account
- 🚩 Notice from customers, victims of identity theft, law enforcement authorities or other persons regarding possible identity theft.

**Contact your Account Manager today for more information!**



## Identity Theft Red Flags Compliance

**How the numbers stack up...**

### Small to Medium Sized Banks:

**50** - Percentage of these banks who say they are close to compliance and will beat the November 1 deadline

**47** - Percentage of these banks who say they either will barely meet the deadline, won't make it or don't know

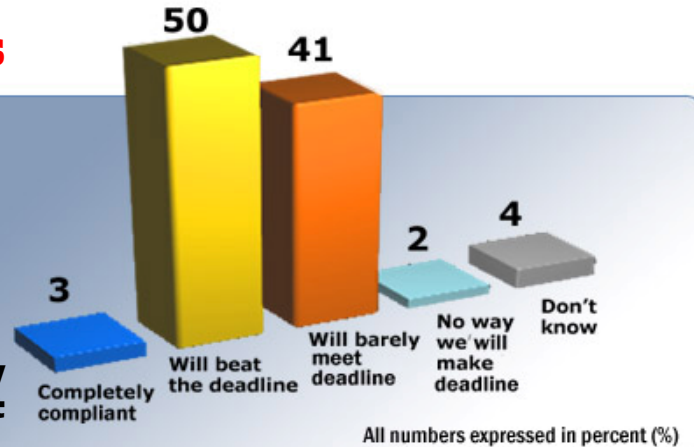
**3** - Percentage of these banks who say they are already completely compliant

### Larger Banks (those with \$2 billion or more in assets under management):

**36** - Percentage of these banks who say they are close to compliance and will beat the November 1 deadline

**61** - Percentage of these banks who say they either will barely meet the deadline, won't make it or don't know

**3** - Percentage of these banks who say they are already completely compliant

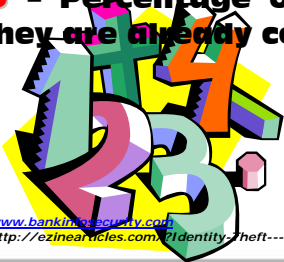


## Could **you** be a victim of Identity Theft?

- 🔥 You check your credit reports annually and find there are new charge cards showing with companies you don't know.
- 🔥 You receive a bill for a credit card account you didn't open.
- 🔥 You notice charges on your credit card statement you did not authorize.
- 🔥 You haven't received your bills or credit card statements when they normally arrive.
- 🔥 Your bank statements show unauthorized transfers or withdrawals.
- 🔥 You receive a call from a collection agency about an account you never opened.
- 🔥 You receive calls from businesses about merchandise you didn't buy.
- 🔥 You're denied credit because debts show up on your credit reports that don't belong to you.

If you notice any of these red flags, don't panic - there may be a logical explanation. But DO follow up on it right away. If it appears you may be a victim of identity theft, go to <http://understandingidentitytheft.com/articles/article-67.html> for a list of steps you should take immediately to rectify the situation.

Source: [www.banklinesecurity.com](http://www.banklinesecurity.com)  
 Source: <http://ezinearticles.com/?Identity-Theft---Red-Flags-That-May-Indicate-Youre-a-Victim&id=112923>



AaSys

Solutions

## IMPORTANT!

**If you require onsite technical support, please remember to call our Service Desk directly to ensure that your request is properly documented and a Service Ticket is opened. To contact Service, please call 800-852-7091 or 813-246-4950.**

*Please join AaSys in welcoming the following individual to our Team:*

**André Saunders,  
Help Desk Engineer**



*AaSys will be closed on Monday,  
September 1, 2008 in observance of Labor Day.*

*Sorry We're*  
**CLOSED**

*Are there topics that you would like to have covered in future newsletters? We are always looking for topics of interest. We welcome all suggestions! To submit a topic, subscribe, or unsubscribe to our distribution list, please email Shama Renée-McIntosh at [smcintosh@aasysgroup.com](mailto:smcintosh@aasysgroup.com).*