By Mark Pribish, Vice President and ID Theft Practice Leader, Merchants Information Solutions, Inc.

Most people believe ID Theft is only a problem for individual consumers.

However, the current environment of cybercrime, data breaches and the insider threat have put a target on the backs of small businesses – where **small business identity theft and fraud has become a new and emerging risk management issue.**

So let's begin with what we know:

- **Small Businesses handle sensitive customer and employee information** including social security numbers, driver's license numbers, birth dates, and bank/credit union account information.
- **Small Businesses use** e-mail, computerized accounting, electronic procurement, and stores electronic employee and customer information.

Now here is some information you may not know:

In 2012, a number of research reports and surveys highlighted how Small Business ID Theft and Fraud has become a new and challenging risk for small business owners including:

- **March 2012 Verizon Data Breach Investigations Report** – found that nearly 75 percent of data breaches analyzed were businesses of 100 employees or less.
- **June 2012 Shred-it Small Business Survey** – reported that security breaches within small businesses are on the rise.
- **October 2012 NCSA / Symantec National Small Business Study** – revealed that U.S. small business owners have a false sense of cybersecurity as 77 percent say their company is safe from cyber threats yet 83 percent have no formal cybersecurity plan.

If you own a small business, the three main things you need to understand are:

Small Business ID Theft Risks such as the loss of business account information such as the Employer Identification Number (EIN) or business bank account information as well as employee or customer data (e.g. credit card number, checking account number, social security number, driver's license number).

This sensitive information can be used to initiate unauthorized activities that appear to be in the

name of the business and/or employee and customers. It is quite similar in concept to personal identity theft except that small businesses DO NOT receive the same consumer protections as individual consumers.

Regulatory and Data Security Laws including The FACT Act, the Red Flags Rule, the HIPAA HITECH data breach requirements and the
46 State Security Breach Notification Laws.

If your small business experiences a data breach, you will most likely have to respond to one or all of the above state and federal laws. Failure to comply is illegal, and can result in fines and penalties negatively affecting your business.

Enterprise Risk Management because no matter whether your company has one person or ten, your legal and financial liability – in the event of a data breach – could be the same as a Fortune 500 company.

It's up to you to protect your business from the threat of identity theft. These are some basic risk management actions that you can take:

- Implement an enterprise risk management (ERM) approach in running your small business
- Increase employee awareness on information security and governance
- Increase employee awareness of ID Theft and Data Breach events
- Understand what type of customer and employee data is being collected and stored
- Implement baseline safeguards and controls including a document retention and destruction policy
- Be vigilant against insider threat, including using pre-employment screening