Data Security and Storage

If you keep it, physically secure it.

Paper records with personal information should be locked, and computer terminals password-protected.

Place your computer server(s) in a secure, controlled location, and keep other devices (e.g. back-up CDs or tape drives) locked away.

Physically lock up all laptops to prevent thieves from walking away with one.

Keep customers and other non-authorized personnel out of private and secure areas.

Instruct employees to save data to network drives where these are available and not to "C:" hard drives, which are much less secure. Should someone steal the hard drive, information stored on network drives remains protected.

Do not copy whole databases to devices when a partial list will do.

Do not put modems/local area network (LAN) cards in computers that do not need them.

Consider an alarm system, preferably one monitored by a security company. Your business insurer may be able to assist you with a security assessment of your operations.

Prevent unauthorized photocopying.

When You Upgrade the System, Upgrade the Security Process*

where hard drives would be disposed, the office should decided to remove the hard drives altogether and have them destroyed.

Virus Protection

Install anti-virus protection software on all computers, and scan your systems for viruses regularly. Never disable anti-virus software, and update it frequently.

Firewalls

Firewalls should be installed at every point where the computer system touches other networks - including the Internet, a customer's system or a telephone company switch. They protect against unauthorized access to information. Ask your Internet Service Provider about other filters that can be used.

Install security "patches"

Most software manufacturers release updates and patches to their software to fix bugs that can allow would-be attackers to gain access to your computer. Check with the manufacturer for new patches or to install automated patching features.

Shred all confidential waste, including payment card information and photocopies of ID documents.

Clean desktops every night.

Only access databases when authorized.

Lock systems when not in use.

Monitor threats

Have your information officer or a key employee track potential security threats and technology updates and report these to employees and managers as needed.

Fraudulent document training

Train employees how to detect fraudulent identity documents.

Network access

Only give access to networks to employees on a need-to-know basis. When an employee leaves, remove their network access immediately.

Evolve Your Practices

Over time, the information your business collects will change. So will your computer technology, databases and personnel. Ensure that you consider how any changes in your operations will affect your management of personal information.

* Sidebar stories in this document are based on actual breaches, but all names, places and other details depicted are fictitious.