Maryland Attorney General's Office
200 St. Paul Place, Baltimore, MD 21202

Brian E. Frosh, Attorney General

Digital Copiers Could Be An Identity Theft Threat

The innocent looking photocopier in the corner of your office could be a potential wealth of information for identity thieves, whether it is still being used at your office or is resold to a third party. How? Similar to computers, hard drive installations have become routine for midsize to large photo copiers, especially those built since 2005. These digital photocopiers are the ones commonly found in businesses and offices. The hard drive stores an image of any document that has been scanned or copied, and the unencrypted data remains until the hard drive is full. When the hard drive becomes full, it simply overwrites old files with newer files.

Many photocopiers use a modem and are connected to an office network. Although they may place passwords on computers, businesses fail to realize the need to protect their copiers as well. Unfortunately, there are serious security issues for data on hard drives, whether the hard drive is in a computer or a copier. Web savvy hackers could access the security network, and gain access to the hard drive with no or easy-to-guess passwords.

Maryland business owners and office administrators have several options to protect the stored data:

- **"Disk Scrubbing."** Businesses can purchase software that scrubs the disk or removes all the data from hard drives. This prevents even the smartest cyberthief from finding any data to steal.
- **Encryption software.** Software to prevent data from being stored at all or to encrypt data can be found online. Some photocopier manufacturers, such as Sharp or Xerox, offer packages with their products.
- **Passwords.** Place a password on the copier that cannot be easily guessed, such as a numerical password similar to a PIN. The copier would then require the password to gain access to the stored data.

Maryland's Personal Information Protection Act (PIPA) requires businesses that maintain personal information to protect that information and dispose of it in a manner that renders it unreadable. Disposing of a photocopier with personal information stored on the hard drive would violate that obligation and expose consumers' personal information. PIPA was enacted to make sure that Maryland

consumers' personal identifying information is reasonably protected. "Personal information" includes an individual's first and last name in combination with a: Social Security Number, Driver's License Number, Financial Account Number or Individual Taxpayer Identification Number. A business that keeps electronic records of its customers' personal information must use reasonable measures that are appropriate to the nature of the personal information and the nature and size of the business. A business disposing of paper records that contain personal information must take reasonable steps to destroy the records in a way that will prevent unauthorized access to or use of the personal information.

In addition to violating PIPA, improperly disposing of consumers' personal information could be considered a security breach. In the event of a security breach, notice must be given to consumers as soon as reasonably practicable following an investigation. Notice to affected consumers must be given in writing and sent to the most recent address of the individual, or by telephone to the most recent phone number. The notice sent to consumers must also include the following:

- Description of the information compromised.
- Contact information for the business, including a toll-free number if the business has one.
- Toll-free numbers and addresses for each of the three credit reporting agencies: Equifax, Experian and TransUnion.
- Toll-free numbers, addresses and websites for the Federal Trade Commission (FTC) and the Office of the Attorney General (OAG).
- A statement that the individual can obtain information from these sources about steps to avoid identity theft.

The business is required to notify the consumer and the OAG. Include a brief description of the nature of the security breach, the number of Maryland residents being notified, and what information has been compromised. Attach a sample copy of the notice being sent to consumers and send to the OAG:

- U.S. Mail:
  Office of the Attorney General
  Attn: Security Breach Notification
  200 St. Paul Place
  Baltimore, MD 21202
- Fax:
  Attn: Security Breach Notification
  410-576-6566
- E-mail:
  idtheft@oag.state.md.us

For more information on your business' obligations to protect personal information, please contact Jeff Karberg, Administrator of the Identity Theft Program at 410-576-6574. Businesses may also go to http://www.oag.state.md.us/idtheft for more information on identity theft.