Privacy Matters – Preventing Identity Theft
Elizabeth Milito, NFIB Legal Foundation

In an age where identity theft has become a widespread occurrence, protecting the privacy of consumers, employees, and applicants has become an important issue. Small-business owners are private citizens as well as business owners. Both consumer roles encourage them to be concerned about privacy.

Although many small-business owners agree that protecting personal information is an inherently a good thing, especially when it comes to medical and financial records, there is concern that privacy legislation could become so broad that it could restrict the ability of a small-business owner to provide personalized customer service or market to an existing customer base. Nevertheless, a sound majority of small employers concerned about the loss of privacy feel the government should err on the side of privacy over economic efficiency if a trade-off is required.

The federal government has passed several laws that impact how you may use and destroy business and personnel records. The penalties for violating privacy laws are steep, carrying both civil and criminal sanctions. To avoid legal problems, make sure you take the appropriate measures regarding the collection and destruction of personal information obtained from customers and employees.

Business Records

Over 60% of small-business owners develop and maintain lists of customers or prospective customers in an attempt to provide more efficient customer service. However, certain laws now influence how much information businesses can collect and from whom they can collect this information.

The Children's Online Privacy Protection Act of 1998 (COPPA) prohibits businesses from collecting personal information online from children who are under 13 years of age. In order to collect such information, businesses must obtain verifiable approval from the child's parents.

The Fair and Accurate Credit Transactions Act (FACT Act) limits the amount of information that can appear on a credit or debit card receipt and requires the proper destruction of information. Only the last five digits of the card number may appear on the receipt, while the expiration date must be omitted completely. Once collected, credit reports must be destroyed in a manner that would make it impossible to reconstruct or read the reports. Acceptable forms of destruction are burning or shredding. Electronic files must be erased.

Personnel Records

Consumer records are not the only documents prone to identity theft. Many employment documents contain sensitive information valuable to identity thieves. To maintain the

privacy of employees and applicants, you must disclose how personal information, such as consumer reports, may affect employment opportunities. You must also disclose information about company-sponsored health plans. Businesses must also take the appropriate steps to destroy this information.

The Fair Credit Reporting Act (FCRA) attempts to promote accuracy in consumer reports and helps ensure the privacy of the information included in them. Subject to state law restrictions, businesses are allowed to use consumer reports during the hiring and evaluation processes, provided the individuals agree to the usage of this information. Individuals must also be notified if information in their consumer reports may negatively affect their employment opportunities.

The Health Insurance Portability and Accountability Act (HIPAA) protects health insurance coverage for workers and their families when they change or lose their job. Health care providers and health care insurers must maintain the confidentiality of all personal information while it is stored and ensure its proper destruction.

Avoiding Potential Problems

Violation of these laws could lead to monetary penalties, prison sentences, and civil lawsuits. To prevent identity theft in your business and avoid legal trouble:

Create a privacy statement and policy for your website to inform consumers about what will happen to the information they provide online.
Include a privacy statement in your employee handbook notifying employees that the company retains the right to access all company property, including computers, desks, and files, at any time. For a model statement, go to the NFIB Legal Foundation's Model Employee Handbook for Small Business, available at http://www.nfib.com/page/legalFoundation.
Notify the applicant in the job application that you will be requesting sensitive information such as a reference check, driving record or criminal background check and obtain an applicant's written consent. Retain the application and consent for the duration of employment plus a minimum of five years. Limit background and reference checks to issues relating to the performance of the job in question. Avoid credit checks unless the employee will be handling money. The EEOC has found that use of credit information may discriminate against minority groups.
Invest in a shredder to destroy all documents that contain personal information.