

FTC ready to set data safeguards

By **Russ Wiles** - Jul. 19, 2009 12:00 AM
The Arizona Republic

When it comes to identity theft, ignorance is no longer bliss.

Many businesses that handle sensitive personal information about customers, patients, employees, suppliers and others will have to develop plans to safeguard the data and resolve problems - or face the consequences.

Starting Aug. 1, the Federal Trade Commission will require businesses, non-profit groups and other entities to draft identity-theft preparedness policies and put them in writing. Entities that fail to do so could face fines of up to \$3,500 per ID-theft incident, not to mention the usual threats of lawsuits and reputational damage that sometimes result from a data breach.

The new rules won't apply to all businesses, but they will pertain to many that collect and store information about others - names, addresses, Social Security numbers, bank-account and credit-card numbers and so on - either because the firms defer payments themselves or bill customers later for goods or services.

Presumably, that would include most companies.

"These days, it is almost impossible to be in business and not collect or hold personally identifying information . . . about your customers, employees, business partners, students or patients," noted the FTC in a statement.

The list of affected entities could include retailers, medical firms, utilities, government agencies, trade associations, debt collectors and charities.

"It really could apply to a big number of businesses," said Janna Day, an attorney at Fennemore Craig in Phoenix.

Many of the provisions were originally designed for banks, lenders, credit-card issuers and others on the front lines of the ID-theft war.

"Financial institutions already are dialed into this stuff, but smaller companies in other businesses might not be," said Elan Mizrahi, a partner at Jennings, Haug & Cunningham in Phoenix.

"It's a broad program that can apply to so many businesses and institutions, in so many ways."

The new regulation, authorized under the Fair and Accurate Credit Transactions Act, aims to cut down on identity thefts, for which Arizona is the per capita leader.

The new rule has two main goals, Day said.

"It aims to protect existing customers' information and make companies more aware of the red flags," including their own vulnerability, she said.


The rule was supposed to take effect late last year but was delayed because of confusion and lagging awareness.

A written ID-theft plan needn't be cumbersome or lengthy, but it should spell out reasonably comprehensive policies. It also needs to be approved by a company's directors or senior management.

A plan needs to cover four areas. An entity must identify fraud "red flags" that are likely for its particular business, devise ways to spot them in practice, take steps to minimize damage and periodically review policies.

A plan might include the naming of an information-security chief, the development of form letters for notifying customers in case of a breach, staff-training

procedures and other details.



Business owners thus would be wise to regard the new policy not as another government-regulatory burden but as an opportunity to formalize an ID-theft policy that could prevent a lot of grief later.

procedures and other details.

Red flags are suspicious patterns, practices or activities that point to fraud, such as someone trying to open an account using a questionable ID card.

It's important to note that a plan should be active and ongoing, in part because ID thieves change their tactics.

"You can't just draft something and file it in a drawer," Day said.

While the requirements don't involve consumers directly, business leaders might be heartened to realize the public supports business efforts to combat ID theft.

A survey released this month by Javelin Strategy & Research found that consumers want to protect their identities and are eager to work with companies to guard them.

Business owners thus would be wise to regard the new policy not as another government-regulatory burden but as an opportunity to formalize an ID-theft policy that could prevent a lot of grief later.

*Article excerpt courtesy of
money.azcentral.com.*