Farmers of Salem
The Salem Oak℠
Insurance since 1851

WHY DO SMALL BUSINESS OWNERS NEED TO PROTECT THEIR BUSINESS AND REPUTATION?

WHAT IS DATA COMPROMISE?

Personal data compromise is the loss, theft, accidental release or accidental publication of personal information. Personally identifying information is generally information that is not available in the public domain, such as name and address in conjunction with an account number.

HOW IS DATA BREACHED?

Data can be breached intentionally through physical theft or electronic hacking; or it can be inadvertently released, such as lost files and exposure on a non-secure website; or it can be fraudulently obtained by data thieves.

WHO CAN BE AFFECTED BY A DATA BREACH?

Current, former, and prospective:

- Employees
- Customers
- Directors
- Clients
- Members

ARE YOUR INSUREDS AT RISK?

- Do they collect personal information on employees or customers, such as account numbers (credit card, checking, etc.), Social Security numbers, or insurance information?
- What would they do if there was a data breach?
- How much would legal assistance cost?

DATA COMPROMISE PROVIDES FIRST-PARTY COVERAGES FOR SMALL BUSINESSES TO RESPOND TO STATE NOTIFICATION REQUIREMENTS

Provides costs for:

- Professional legal counsel to review the facts and advise on the appropriate course of action.
- Information technologies to review the nature and extent of the data breach.
- Notification to affected individuals – typically involving the creation of a package of materials that is mailed to the individuals affected by the breach.
- Public relations services includes costs to implement public relations recommendations, including advertising and special promotions.

THIRD-PARTY COVERAGE (OPTIONAL)

Third-party coverage is available to protect the insured from lawsuits filed by affected individuals upset about the data breach when their private information is exposed.

DATA COMPROMISE PROVIDES ADDITIONAL BUSINESS REPUTATION PROTECTION

In addition to the various state notification requirements, it is expected that an entity suffering from a data breach will provide services to those affected by the breach. Failure to provide such services may further damage a business's reputation. In the event of a data breach, Data Compromise coverage provides expense reimbursement for the following at no cost to those individuals affected by the breach:

- **Packet of Informational Materials** containing loss prevention and customer support information.
- **Toll-Free Help-Line** for those affected by the breach to call with questions pertaining to the breach.
- **One year of Credit Monitoring** for up to 12 months from the date of notification.
- **Identity Recovery Case Management Services** for those affected by the breach who have had their identity stolen as a result of the breach. Services are to be initiated within 12 months of the notification and may continue for 12 months from the date of initiation.

The services listed above can be tailored by the insured depending on the size of the breach and the type of data breached.

OPTIONAL COVERAGE IS AVAILABLE FOR DEFENSE AND LIABILITY

Defense and Liability is provided should insured receive notice of a data compromise suit brought by one or more "affected individuals" or by a governmental entity on behalf of one or more "affected individuals".

THE RISK FOR DATA COMPROMISE IS REAL

1. STOLEN LAPTOPS

A laptop was stolen from the office of a primary care physician. The stolen computer contained information on 255 former and current patients, including their names, dates of birth, Social Security numbers, medical records and payment information.

2. DUMPSTER DIVING

A ring of methamphetamine addicts was scavenging through specific dumpsters located outside of retail stores and food shops for credit card information, transaction receipts and account statements. None of the information was shredded. The identity theft ring included a computer security technician and an internet service provider (ISP) employee.

3. COMPUTER THEFT

A burglar stole a computer from an insurance agent's office containing the personal information of 800 current and potential clients. The information stolen included Social Security numbers, bank account and credit information.

4. UNSECURED COMPUTING

An employee of an accounting firm used a company computer to trade music via a file-sharing computer application. The employee exposed clients' private files, including bank account and routing information and Social Security numbers, to identity thieves using the website's peer-to-peer network. Investigators found that personal information on 2,000 clients was downloaded by dozens of users, some outside the United States.

5. DATABASE HACKING

Data thieves hacked into the database of an apartment leasing company. The company's database contained personal information about 100 tenants and another 275 applicants. Information included Social Security numbers, employment and credit information.

As of October 2015, fifty U.S. jurisdictions – 47 states plus the District of Columbia, Puerto Rico and the U.S. Virgin Islands – now have laws requiring notification of individuals whose personal information is lost or stolen.

Additional Coverage Highlights

Limits: $50,000 annual aggregate.
Increased limits of $100,000, $250,000 may be available pending a short questionnaire

- Forensic Technology Review: $5,000 sublimit
- Legal Review: $5,000 sublimit
- Public Relation Expenses: $5,000 sublimit
- Named Malware: $50,000 sublimit.

Deductible: $1,000.

Be aware of the information you collect, how you use it and how you store it. It's your responsibility and your business's reputation on the line.