Employment Practices Liability & Cyber Liability and Data Security + Instant Quote

Employment Practices Liability provides coverage for claims involving discrimination, wrongful termination and harassment. **Cyber Liability and Data Security+** provides coverage for data breach liability, data breach expense, website liability and identity theft expense.

Please complete the information below to obtain quotes for these two, separate products. A fully completed application, signed and dated by the applicant, will be required to confirm each quote.

INSTANT QUOTE INFORMATION

1. Name of applicant: _____State _____ Zip: _____
2. Nature of business: _____
3. Web address: _____
4. Number of employees:
   a. Full time, including independent contractors & leased _____
   b. Part time, including temporary & seasonal _____
5. Annual receipts for most recent 12- month period: _____

Coverage cannot be bound using this form. Premium, limits of liability, terms, conditions and eligibility for coverage may change based on any additional information provided in a full submission for any individual risk. Binding of any quote is subject to underwriter receipt, review and acceptance of completed, signed and dated USLI applications for these products and any other required subjectivities.

ELIGIBLE CLASSES:

Eligible classes for both the Cyber Liability* and Employment Practices Liability products (including but not limited to):

Advertising firm	Day care center	Nonprofit entity
Architect	Day spa	Permanent placement employment agency
Artisan contractor	E-commerce	Plumber
Auto repair	Engineer	Printer/Publisher
Beauty/barber/nail shop	Fast food restaurant	Property manager
Bowling lane	Fitness center	Real estate agency
Camp	Furniture rental	Rental car agency
Catering service	Hotel/Motel	Retail store
Cemetery	Insurance agency (Cyber only for USLI appointed agents)	Sales/Distributor
Claims adjuster		Security guard firm
Consultant	Landscaper	Supermarket
Convenience store	Maintenance	Transportation/Trucking
Country club	Manufacturer (non-information technology)	Travel agency

Eligible classes for Cyber Liability* only (including but not limited to):

- Bar/Tavern
- Entertainment industry
- Restaurant with table wait staff
- Telemarketing

* No medical or financial services companies.

ABRAM INTERSTATE INSURANCE SERVICES, INC.
2211 Plaza Drive, Suite100
Rocklin, CA 95765
Phone: 916.780.7000 Fax: 916.780.7181

Cyber Liability and Data Security+

DID YOU KNOW:

- A study by a major credit card company found that 85% of all data breaches occur at the small business level.
- Organized crime considers small businesses to be low risk, high reward targets.
- Small business owners are popular targets of identity thieves because they have larger lines of credit, higher volume of transactions and valuable computer networks.
- Common reasons personal information is breached include criminal hacking, lost or stolen laptops, computers, or paper reports and negligent or malicious employee activity.
- It is illegal for business owners to not report and not send notification to those whose legally protected personal information is breached.

WHAT ARE THE COSTS OF DATA BREACHES?

- Claims for failure to protect information, expense of legally required notifications and credit monitoring to those whose information is exposed, forensic expense to find out and resolve what happened, public relations expense to maintain business reputation, regulatory and payment card industry fines and hacker extortion demands.
- In 2011, the average cost to business owners per record compromised was $194.
- Small business owners have gone out of business due to identity thieves impersonating their business and personal name leading to loan defaults, inability to access credit and loss of business reputation.

USLI can help protect you with the following product features:

COVERAGE FEATURES	OUR GROUP	COMPETITORS' POLICY
Separate aggregate limits of liability per Coverage Part with option to combine into one aggregate limit.	✓	?
Liability arising from both Data Breach & Security Breach	✓	?
Data Breach Expense and Identity Theft expense paid as incurred (pay-on-behalf) instead of by reimbursement	✓	?
Defense of Regulatory Proceedings	✓	?
Payment Card Industry (PCI) Fines & Penalties	✓	?
Data Breach Expense coverage including notification letters, public relations, forensics & credit monitoring	✓	?
Cyber Extortion Expenses	✓	?
Website Liability including libel, slander, misappropriation of ideas, plagiarism, piracy, copyright & trademark violations	✓	?
Identity Theft expense including credit monitoring & expense to retain specialists to resolve identity theft for board members and owners	✓	?
Access to the Business Resource Center which provides free and discounted business solutions to USLI policy holders.	✓	?

ABRAM INTERSTATE INSURANCE SERVICES, INC.
2211 Plaza Drive, Suite100
Rocklin, CA 95765
Phone: 916.780.7000 Fax: 916.780.7181

CYBER LIABILITY AND DATA SECURITY + FOR INSURANCE AGENTS

Claim Examples

Coverage Part A

- **Data Breach Liability:** Alice owns an agency that was not yet paperless. She hired a few interns over the summer to scan everything electronically in order to prepare for the new agency management system. Over those four months, some insureds became victims of identity theft and paid for their own credit monitoring; others' bank accounts slowly drained, and they were not able to recover stolen funds because too much time had expired without their noticing the fraudulent activity. Since some bigger net-worth clients were affected, an investigation was conducted. It was later found that one of the interns had stolen the personal information contained on the applications and other files at the agency and sold the identities online. Victims banded together and sued the agency for costs incurred, including paying for credit monitoring, recovering lost funds and expenses incurred in clearing their identities.

- **Security Breach Liability:** Diane's insurance agency is sued by an e-commerce organization for its participation in a denial of service attack against the e-commerce firm. Diane's agency had antivirus and firewall protection on its computers; however, the firm had not made updates to them in the past couple years. It turns out their computers became infected with malware, which, when activated, participated in an attack against the e-commerce firm's servers, overloading them with requests and shutting down their system for a day. The e-commerce firm sued the agency, among others for lost revenue and costs to repair their server as a result of the neglect of standards of care by those unknowingly participating in the attack. Diane's agency paid over $50,000 in defense and settled for $30,000 in loss.

- **Defense of Regulatory Proceedings:** Joe owns an insurance brokerage. Joe makes the decision to store client names, addresses, phone numbers and email addresses to cross-sell other products. The brokerage does not have proper security in place to protect the information. A hacker gains access to the personal information and sells it on the Internet. The state where the merchant is located accuses them of privacy law violations and sets up hearings to decide if fines will be assessed. Joe expends $10,000 to defend the company and is ultimately fined $30,000.

Coverage Part B

- **Data Breach Expense:** An insurance retailer is hit with a data breach, exposing the social security numbers of a large number of customers. State law requires the retailer to report the breach and notify the customers. The retailer spends over $400,000 to hire a firm to conduct forensics to determine all those affected, re-secure its network, send out notification letters across multiple states and set up credit monitoring for the customers. In addition, $75,000 is spent on hiring a public relations firm to manage the publicity surrounding the event.

- **Cyber Extortion Threat Expense:** Jerry, the president of an insurance agency, arrives at work to find he and his employees are locked out of the computer system. A hacker notifies him that they have 24 hours to pay $10,000 or all files on the server will be deleted. As the deadline nears, Jerry realizes that he cannot thwart this attack, and he is forced to pay the amount demanded.

Coverage Part C

- **Website Liability:** An insurance agency posts coming attractions links on its Website to a new movie. The coming attractions contain many scenes of car crashes, and the agency uses this as a fun way to sell auto insurance; however, the agency never received permission to post these images. Several movie studios threaten lawsuits based on violations of intellectual property. At first, the agency fights but then relents, agreeing to take down the postings after spending $10,000 in defense costs.

- **Website Liability:** Mike is a broker along the Florida coast. He has a social media page instead of a Website which includes a section for customer feedback. Mike monitors posts daily and is shocked to find a review from an insured who stated that his service was awful, premium was too high and the company never paid her claim. Mike posted a reply to the insured saying she was the one who insisted on using that carrier even though he recommended something less expensive, she was rude and confrontational and that of course the carrier denied her claim because “crazy” was not a covered cause of loss. The insured sued for $1,000,000 for libel and intentional infliction of emotional distress.

Coverage Part D

- **Identity Theft:** Carl is a small business owner of a local insurance agency looking to expand his operation. When Carl inquired about a loan to open up a new location, the bank turned him down for poor credit. Apparently, his identity was stolen, and the thief had opened up additional lines of credit and was purchasing big ticket items such as a car and boat. They all went unpaid, and collection attempts went to a fake address set up by the thief. Carl’s operation is now headed toward bankruptcy, as he cannot dedicate time to his business while he tries to clear his credit record, nor can he access credit to keep the business going.

ABRAM INTERSTATE INSURANCE SERVICES, INC.
2211 Plaza Drive, Suite100
Rocklin, CA 95765
Phone: 916.780.7000 Fax: 916.780.7181

Cyber Liability and Data Security +

Claim Examples

COVERAGE PART A

- **Data Breach Liability:** Alice owns a restaurant whose point of sale machines had been illegally skimmed with a small, hidden electronic device for eight months, affecting nearly 1,000 cards. Over those eight months, some cardholders became identity theft victims, and paid for their own credit monitoring; others had debit cards skimmed and were not able to recover stolen funds from their bank accounts because too much time had expired without them noticing the fraudulent activity. Victims banded together and sued the store for costs incurred, including paying for credit monitoring, recovering lost funds and expenses incurred in clearing their identity.
- **Security Breach Liability:** Diane's real estate agency is sued by an e-commerce organization for its participation in a denial of service attack against the e-commerce firm. Diane's agency had antivirus and firewall protection on its computers; however, the firm had not made updates to them in the past couple years. It turns out their computers became infected with malware, which, when activated, participated in an attack against the e-commerce firm's servers, overloading them with requests and shutting down their system for a day. The e-commerce firm sued the agency, among others for lost revenue and costs to repair their server as a result of the neglect of standards of care by those unknowingly participating in the attack. Diane's agency paid over $50,000 in defense and settled for $30,000 in loss.
- **Defense of Regulatory Proceedings:** Joe owns an appliance sales organization. Joe makes the decision to store client names, addresses, phone numbers and spending habits to help cross-sell their other products. The organization does not have proper security in place to protect the information. A hacker gains access to the personal information and sells it on the Internet. The state where the merchant is located accuses them of privacy law violations and sets up hearings to decide if fines will be asessed. Joe expends $10,000 to defend the company and is ultimately fined $30,000.
- **Payment Card Industry (PCI) Fines & Penalties:** A small family restaurant in Utah was informed by their payment card-processing bank of a potential data breach of their point-of-sale system. A forensics investigation found they unintentionally stored credit card numbers. However, the payment card processor demanded indemnification for fines assessed by the credit card companies who alleged a data breach. The payment card processor withdrew $10,000 from the restaurant's bank account and sued them for the balance of $80,000.