AXIS CYBER RANSOMWARE SUPPLEMENTAL APPLICATION

AXIS INSURANCE
10000 Avalon Blvd. Ste. 200
Alpharetta, GA 30009
Telephone**: (678) 746-9000** | Toll-Free**: (866) 259-5435** | Fax: **(678) 746-9315**
https://www.axiscapital.com/insurance/cyber-technology-e-o

SOLELY AS RESPECTS CLAIMS-MADE LIABILITY COVERAGES UNDER THE POLICY FOR WHICH THIS APPLICATION IS BEING SUBMITTED: THIS INSURANCE POLICY PROVIDES COVERAGE ON A CLAIMS-MADE AND REPORTED BASIS AND APPLIES ONLY TO CLAIMS FIRST MADE AGAINST THE INSURED DURING THE POLICY PERIOD OR ANY APPLICABLE EXTENDED REPORTING PERIOD AND REPORTED TO THE INSURER AS SET FORTH IN THE REPORTING OF CLAIMS AND EVENTS SECTION. DEFENSE COSTS ARE INCLUDED IN THE LIMITS OF INSURANCE, AND PAYMENT THEREOF WILL ERODE, AND MAY EXHAUST, THE LIMITS OF INSURANCE.

ABOUT THIS APPLICATION

- "Applicant" refers individually and collectively to all proposed insureds. All responses shall be deemed made on behalf of all proposed insureds. **If responses differ for any proposed insureds (including subsidiaries) please complete additional supplementals for those.**
- This Application and all materials submitted herewith shall be held in confidence.
- The submission of this Application does not obligate the Applicant to buy insurance nor is the Insurer obligated to sell insurance or to offer insurance upon any specific terms requested.
- If the policy applied for is issued, this Application, which shall include all Supplemental Applications and material and information submitted in connection with this Application, will be deemed attached to and will form a part of the policy.

INSTRUCTIONS

Respond to all questions completely, leaving no blanks. Check responses when requested.

If space is insufficient, continue responses in additional commentary box at the end of the supplemental.

This Application must be completed, dated, and signed by an authorized officer of the entity identified in the section entitled "Applicant Information" on the main Application.

1.0 Governance

Company Name:	Address:	Risk Mgr. Email:

Identify the most senior role with responsibility for information security, such as CISO or equivalent:	
Does this role have direct responsibility for managing security incident response?	☐ Yes ☐ No

To whom does this role report? (Select all that apply)	☐ Executive committee or officers ☐ Principal owners or shareholders ☐ Board of directors	☐ CIO/CTO ☐ CFO ☐ CEO	☐ Other:
How frequently is a formal reporting provided?	☐ Monthly ☐ Quarterly	☐ Semi-annually ☐ Annually	☐ Ad Hoc ☐ Other:
Does the Applicant have a **written information security policy**?		☐ Yes ☐ No	Last updated:
Identify any standards or frameworks the security program is based on: (Select all that apply)		☐ NIST CSF, 800-53, 171 or others ☐ ISO/IEC 27001 ☐ PCI-DSS	☐ CIS 18 ☐ Other:
Peer Sharing Groups: Does the Applicant participate in any information security threat, vulnerability and incident sharing program to improve awareness, assessment, monitoring and response?			☐ Yes ☐ No
Security Management: Are any of the following implemented? (Select all that apply)		☐ Unified threat mgt./prevention systems ☐ Independent security audit or assessment ☐ Managed security services	
Screening: Are applicants screened, including credit history, criminal, drug testing as permitted by law?			☐ Yes ☐ No
Applicant maintains the following documents:			

☐ Business Continuity Plan – Reviewed and tested	☐ Semi-annually	☐ Annually	☐ Other:
☐ Disaster Recovery Plan – Reviewed and tested	☐ Semi-annually	☐ Annually	☐ Other:
☐ Incident Response Plan – Reviewed and tested	☐ Semi-annually	☐ Annually	☐ Other:

Are copies of the above stored and accessible even if the network is unavailable?	☐ Yes ☐ No

Identify IR playbooks in place and tested: ☐ None ☐ Ransomware ☐ Business Email Compromise ☐ Other:

Additional Comments:

How frequently is a formal reporting provided?	☐ Monthly ☐ Quarterly	☐ Semi-annually ☐ Annually	☐ Ad Hoc ☐ Other:

Does the Applicant have a written privacy policy or notice?	☐ Yes ☐ No	Last reviewed by attorney:

2.0 CONTROLS

2.1 Vulnerabilities & Patching	Does the Applicant maintain a documented vulnerability management plan?	☐ Yes ☐ No
If "Yes", does it identify target timeframes for addressing Critical, High, Med, and Low vulnerabilities?		☐ Yes ☐ No

Is application of Zero-day and Emergency patches expedited?	☐ Yes ☐ No	If "Yes", please identify target timeframes:

Please identify the target timeframe for addressing Critical/High vulnerabilities (CVSS 7.0-10.0):	☐ < 24 Hours ☐ 24-72 Hours	☐ 3-7 days ☐ > 7 days
Please identify your standard cadence for addressing Medium or Low vulnerabilities:	☐ < 30 days ☐ 30-60 days	☐ 60-90 days or greater ☐ Ad Hoc only

Does the Applicant receive threat/vulnerability alerts from external sources?		☐ Yes ☐ No
Does the Applicant use a solution to identify vulnerabilities, track remediation and/or identify trends?	☐ Yes ☐ No	If "Yes", please identify solution:

A formal process exists for assessing vulnerabilities potential impact to Applicant's environment:	☐ Yes ☐ No

Indicate frequency of **internal scanning**:	☐ Continuously ☐ Daily	☐ Weekly ☐Monthly	☐ Quarterly ☐ Twice/yr.	☐ Annually ☐ Ad Hoc	☐ Never ☐ Other:

Indicate frequency of **external scanning**:	☐ Continuously ☐ Daily	☐ Weekly ☐ Monthly	☐ Quarterly ☐ Twice/yr.	☐ Annually ☐ Ad Hoc	☐ Never ☐ Other:
Percent of environment covered by scans:			% (If <100% please provide detail in Additional Comments below)		
Additional Comments: (Please give an overview of the Applicant's vulnerability management and critical patching process and timeline, if outside of the above):					

2.2 Pen Testing	The Applicant conducts regular penetration testing? (Select all that apply and frequency below. If 'Other', please provide detail in Additional Comments below).
☐ External-network	☐ Quarterly ☐ 2x/yr. ☐ Annually ☐ Ad Hoc ☐ Never ☐ Other
☐ Internal-network	☐ Quarterly ☐ 2x/yr. ☐ Annually ☐ Ad Hoc ☐ Never ☐ Other
☐ Social engineering	☐ Quarterly ☐ 2x/yr. ☐ Annually ☐ Ad Hoc ☐ Never ☐ Other
☐ Physical	☐ Quarterly ☐ 2x/yr. ☐ Annually ☐ Ad Hoc ☐ Never ☐ Other
☐ Web App.	☐ Quarterly ☐ 2x/yr. ☐ Annually ☐ Ad Hoc ☐ Never ☐ Other
☐ Other:	☐ Quarterly ☐ 2x/yr. ☐ Annually ☐ Ad Hoc ☐ Never ☐ Other
Testing is conducted:	☐ Internally ☐ Outsourced
Additional Comments:	

2.3 Life Cycle & Inventory Mgt:	Does the Applicant use any operating system, hardware or software that is no longer supported or is considered End-of-Life (EoL) by the manufacturer?	☐ Yes ☐ No

If "Yes", please identify the EoL component(s):	If "Yes", please identify their function:

Please indicate the controls applied to EoL components:	☐ Known and Inventoried ☐ Decomm/replacement plans in place ☐ Additional service purchased	☐ Tracked and reported ☐ Monitoring and alerting ☐ Segmented	☐ Other:
Are ALL EoL components covered by controls above:	☐ All covered ☐ Some not covered (Please provide detail in Additional Comments below)		
An up-to-date hardware and software inventory is maintained?			☐ Yes ☐ No
Inventory processes are:	☐ Manual ☐ Semi-automated ☐ Fully automated		

Hardware inventory updates occur:	☐ Continuously ☐ 2x/yr. ☐ Other: ☐ Quarterly ☐ Annually		Percentage of hardware inventoried: %
Percentage of software inventoried?	%	Are users allowed to install applications?	☐ Yes ☐ No
Additional Comments:			

2.4 SOC/SIEM	Does the Applicant use a SIEM?		☐ Yes (please identify the solution in Additional Comments below) ☐ No	
Is the SIEM tuned for your org. with 100% network log coverage?	☐ Yes ☐ No		If any, identify systems whose logs are excluded from SIEM:	
How frequently are logs reviewed?	☐ Continuously ☐ Weekly ☐ Monthly	☐ Quarterly ☐ Semi-annually ☐ Annually	How long are audit logs maintained? At least:	☐ 30 days ☐ 90 days ☐ 1 year or greater
Is a Security Operations Center used?	☐ Yes ☐ No	If yes: ☐ Staffed 24/7/365 "eyes on glass" ☐ Other: ☐ Internal staff ☐ External staff ☐ SOC staff can take responsive or corrective action in event of alert.		
If 3rd party/MSSP, please indicate contractual notification and response time (Days/Hours/Mins):				
If SOC/SIEM not used, please identify alert notification and handling processes:				
Additional Comments:				

2.5 Security Configuration:	Hardened configs are used for:		
	☐ Laptops ☐ Workstations ☐ Mobile devices ☐ Web apps	☐ Servers ☐ Databases ☐ Security applications	☐ Not used ☐ Other:
Security configurations are updated at least:	☐ Monthly ☐ Quarterly	☐ Semi-annually ☐ Annually	☐ Other:

Indicate hardening standards used:	☐ Center for Internet Security ☐ Microsoft ☐ NIST ☐ SANS ☐ Other:
Additional Comments:	
Is software installation automatically controlled and unauthorized software blocked?	☐ Yes ☐ No

2.6 Backups & Redundancy:	Critical back-ups are completed:	☐ Continuously ☐ Weekly ☐ Other: ☐ Daily ☐ Monthly
Which of the following does Applicant utilize for backups?		☐ Tapes ☐ Cloud ☐ Disk ☐ Other:
Back-ups are stored:		☐ On premises ☐ Offline ☐ Offsite ☐ Secondary Data Center ☐ MSSP ☐ Other:
Indicate existing backup controls:		☐ Segmentation ☐ Malware Scanning ☐ Unique Backup Accounts (stored separately) ☐ Encryption ☐ Immutable ☐ Priv. Access Mgt. ☐ Other:
If encrypted, are keys stored offline?	☐ No ☐ Yes	If offline, how often is data moved? ☐Continuously ☐ Weekly ☐ Quarterly ☐ Daily ☐ Monthly ☐ Other:
Full, or large scale, restoration is tested:		☐ Quarterly ☐ Twice annually ☐ Annually ☐ Not tested ☐ Other:
Identify redundancy or resiliency solutions in place:		☐ Hot Site ☐ Warm Site ☐ Snapshots ☐ Failover environment ☐ Other:
Additional Comments:		

2.7 Intrusion Detection & Prevention:	Does the Applicant employ any intrusion detection and prevention solution?	☐ Yes ☐ No
	Review frequency of intrusion logs? At least:	☐ Continuously ☐ Daily ☐ Weekly ☐ Bi-weekly ☐ Monthly ☐ Quarterly
What is the expected time to respond to an intrusion?		Hours: Minutes:

2.8 Malware Detection & Response:	Does the Applicant employ an endpoint detection and response solution (EDR or similar) with behavioral analysis/anomaly detection?	☐ Yes ☐ No
If "Yes", on what % of endpoints is the solution deployed?		Endpoints: % Servers: %
Please identify the endpoint protection solution(s) in place (Company/product name):		

Is the solution tuned to block threats?	☐ Yes ☐ No	Is DDoS mitigation in place?	☐ Yes ☐ No

2.9 Data Loss Prevention (DLP):	Does the Applicant employ a DLP solution?	☐ Yes ☐ No
	If "Yes", identify the solution(s) in place (Company/product name):	
Does the Applicant control the transmission of Personal Information, Corporate Information and Critical Information off network?	☐ Off network ☐ Email ☐ Removable media ☐ Internet/Cloud (data storage sites, message boards, etc.)	
Are removable storage devices monitored and regulated?		☐ Yes ☐ No
Are data threshold alerts in place (exfiltration, deletion, movement)?		☐ Yes ☐ No

2.10 Encryption:	Does the Applicant employ mandatory encryption to protect the following? (Select all that apply)		
☐ Information in transit ☐ Information at rest	☐ Corporate Information at rest ☐ Corporate Information in transit	☐ Critical information ☐ Removable media	☐ Personal devices ☐ Other:

2.11 Email Security:	Please identify the email security controls in place:		
☐ DKIM ☐ DMARC ☐ SPF	☐ Quarantine ☐ Block suspicous senders? ☐ Block malware/phishing/SPAM?	☐ Tag/notify external email ☐ Block malicious attachments/content? ☐ Macros disabled	☐ Sandboxing ☐ Other:

Does the Applicant employ Microsoft (Office) 365?	☐ Yes ☐ No	If yes, is MS365 ATP /Defender used? If yes, what is your MS Secure Score %? %	☐Yes ☐ No
If other cloud-based email system, please identify:			
Additional Comments:			

2.12 Firewalls:	Does the Applicant employ the following firewalls?	☐ External or perimeter ☐ Internal
	Are default passwords changed?	☐ Yes ☐ No
IP filtering is used to prevent connections from known-malicious addresses?		☐ Yes ☐ No
Network ports can only be opened with a legitimate business need?		☐ Yes ☐ No
Port restrictions, configurations, etc. are verified:	☐ Semi-annually ☐ Annually ☐ Ad Hoc ☐ Other:	

What is the firewall policy? (Select all that apply)	☐ Deny all by default, permit by exception ☐ Deny by exception ☐ Other:
Additional Comments:	

2.13 Segmentation:	Are the following segregated in an isolated environment?	☐ Personal Information ☐ Critical servers	☐ Corporate Information ☐ Critical Information

Indicate any existing network segmentation:	☐ Geographic ☐ IT Management ☐ Business Function ☐ Subsidiaries	☐ Guest wireless ☐ Servers ☐ OT ☐ None	☐ Other:
How is segmentation accomplished?	☐ Firewalls ☐ Sep. Domains ☐ VLAN's ☐ Other:		
Are development, testing and production conducted in separate environments?	☐ Yes ☐ No		
Additional Comments:			

2.14 Access:	Is network and information access based on a least privilege basis?	☐ Yes ☐ No

Is a formal process in place for assigning access for all hires, terms, and changes?	☐ Yes ☐ No	If "Yes", is it: ☐ Manual ☐ Semi-automated ☐ Fully automated ☐ Other:
User access is reviewed and updated:	☐ Monthly ☐ Quarterly ☐ Annually ☐ Never ☐ Other:	
Admin/privileged access is reviewed & updated:	☐ Monthly ☐ Quarterly ☐ Annually ☐ Never ☐ Other:	
Does the Applicant impose minimum security requirements on all devices connecting to the network?	☐ Yes ☐ No	
Does the Applicant use a Mobile Device management (MDM) solution that allows remote wipe?	☐ Yes ☐ No	

Passwords: Please identify any required password elements:

☐ Upper/Lower/Special char. ☐ Min. character length 10 or > ☐ Min. character length 9 or <	☐ Expiration every 6 months or less ☐ Check for cracked/common passwords ☐ Lockout after 6 invalid attempts	☐ Dictionary check ☐ Passphrase ☐ Other:
Additional Comments:		

2.15 Domain/Privileged Accounts & Controls	Please identify domain administrator account controls in place?	☐ Separate accts. ☐ PAM/Pwd vault ☐ PAM (Check In/Out) ☐ Priv. Access Workstations	☐ Other:
If PAM or Vault:	• Is a separate MFA instance required to access this? • Are all domain admin accounts (incl. service accounts) maintained in the solution?		☐ Yes ☐ No ☐ Yes ☐ No
Total # of:	Domain Admin. Accounts:	Service Accounts w/ Domain Admin rights:	
If only admin passwords, define requirements:	Min. length: Rotation: Complexity:		
Is all domain admin account activity logged and monitored for unusual behavior?			☐ Yes ☐ No
Are changes to admin/privileged accounts monitored and alerted automatically?			☐ Yes ☐ No
All service accts have interactive login disabled?	☐ Yes ☐ No (If "No", indicate # of accounts with login enabled and why):		
Indicate number of users with Local Admin rights on their systems (Please provide detail in Additional Comments below)	☐ All ☐ No controls in place ☐ LAPS or similar control in place ☐ None ☐ Limited # of users ☐ Other:		
Additional Comments:			

2.16 Access	MFA is required for the following access: (Please provide detail in Additional Comments below, if needed)		
☐ All Admin/Privileged access (On-prem AND remote) ☐ All access to cloud-based solutions ☐ All remote access into network ☐ Remote access by vendors/contractors		☐ Access to backups ☐ Access to Remote Desktop Protocol or similar ☐ Access to cloud email (i.e.:MS365) ☐ Other:	
What MFA methods are in use?	☐ Secondary Email ☐ SMS/Text ☐ Biometrics	☐ Authenticator App ☐ Physical keyfob/card ☐ Other:	☐ Endpoint Cert. (Please indicate where used in Additional Comments below)
Additional Comments:			

Wireless: Does the Applicant maintain wireless security policies:			☐ Yes ☐ No		
Are connections from untrusted wireless devices allowed?	☐ Yes ☐ No	If "Yes", do untrusted wireless devices use a separate network?	☐ Yes ☐ No		
2.17 Training & Awareness:	Annual training is required for:	☐ Employees/ Contractors ☐ Vendors ☐ Ad hoc only ☐ Not Required	Please indicate topics:	☐ Threats ☐ Social Eng. ☐ Privacy ☐ Role-based	☐ Regulations/ Policy ☐ Phishing ☐ Data Handling ☐ Other:
Are Phishing simulations conducted for all employees?	☐ Yes ☐ No	If "Yes", indicate frequency:	☐ Monthly ☐ Twice Annually ☐ Ad Hoc ☐ Quarterly ☐ Annually ☐ Other:		
Are Phishing Simulations:		☐ Role Based ☐ Targeted ☐ Staggered			
What % of staff are covered in each simulation?		☐100% ☐25% or less ☐25 to 50% ☐50 to 75% ☐Other:			
Click rate of most recent simulation:		☐ <5% ☐5-10% ☐ 10-15% ☐15-20% ☐ >20% ☐Other:			
What is the most recent reporting rate?		☐ <5% ☐5-10% ☐ 10-15% ☐15-20% ☐ >20% ☐ Other:			
Does the Applicant require additional training on failure?			☐ Yes ☐ No		
Does the Applicant have a report phishing email add-in enabled for all email users?			☐ Yes ☐ No		
Does the Applicant employ a sandboxing solution for investigating suspicious emails/attachments?			☐ Yes ☐ No		
Is information security and privacy training content reviewed at least annually?			☐ Yes ☐ No		
Are service providers/3rd parties with access to the network required to take this training annually?			☐ Yes ☐ No		
Additional Comments:					

2.18 RDP/SMB	Is RDP or other remote connection solution enabled?	☐ Yes ☐ No
If "Yes", is RDP or other accessible:	☐ Internally ☐ Externally (public) ☐ External only after remote connection/VPN	
Indicate additional controls:	☐ Restricted to IT personnel ☐ Sep. accounts required ☐ Network authentication ☐ Alerting and monitoring for each use ☐ Accessible through PAM ☐ Other: ☐ Lockout after failed attempts	

Additional Comments:		
2.19 Vendor Review	Does the Applicant have a vendor review process that includes periodic review of third parties:	☐ Security Program ☐ In/External assessments ☐ Data provided ☐ Services/changes ☐ Tech. changes ☐ Leadership changes

REPRESENTATIONS AND SIGNATURE

By signing this document, the undersigned authorized representative of the Applicant represents on behalf of all persons and entities proposed for coverage, after inquiry, that to the best of their knowledge:

1. The statements and answers given in and all materials submitted with this Application are true, accurate and complete.
2. No facts or information material to the risk proposed for insurance have been misstated or concealed.
3. These representations are a material inducement to the Insurer to provide a proposal for insurance.
4. Any policy the Insurer issues will be issued in reliance upon these representations.
5. The Applicant will report to the Insurer immediately in writing any material change in the Applicant's activities, products and services.
6. The Applicant will report to the Insurer immediately in writing any material changes to the answers provided in this Application which occur or are discovered between the date of this Application and the effective date of the policy for which coverage is sought by submission this Application.
7. The Insurer reserves the right, upon receipt of any such notice, to modify or withdraw any proposal for insurance the Insurer has offered.

WARNING

PLEASE REVIEW THE STATE FRAUD STATEMENT CONTAINED AT THE END OF THIS APPLICATION APPLICABLE TO THE STATE IN WHICH THE APPLICANT RESIDES.

Any person who, with intent to defraud or knowingly facilitates a fraud against the insurer, submits an application or files a claim containing a false or deceptive statement may be guilty of insurance fraud.

AXIS CYBER RANSOMWARE SUPPLEMENTAL APPLICATION

This Application must be signed by the Applicant's Chief Executive Officer, President, Chief Information Officer, Chief Technology Officer, Chief Security Officer, Chief Operating Officer, Chief Financial Officer or General Counsel or Risk Manager, or their functional equivalent, unless the Insurer instructs the Applicant otherwise.

Name _____ Name (Signature) _____

Title _____

Date _____

TO BE COMPLETED BY PRODUCERS ONLY:

RETAIL PRODUCER		WHOLESALE PRODUCER	
Producer Name: **City, State:** **Telephone No.:** **License No.:**		**Producer Name:** **City, State:** **Telephone No.:** **License No.:**	

Producer Signature: _____

STATE FRAUD STATEMENT

ALABAMA

Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or who knowingly presents false information in an application for insurance is guilty of a crime and may be subject to restitution fines or confinement in prison or any combination thereof.

ARKANSAS

Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

CALIFORNIA

For your protection, California law requires the following warning to appear on this form: Any person who knowingly presents false or fraudulent information to obtain or amend insurance coverage or to make a claim for the payment of a loss is guilty of a crime and may be subject to fines and confinement in state prison.

COLORADO

It is unlawful to knowingly provide false, incomplete, or misleading facts or information to an insurance company for the purpose of defrauding or attempting to defraud the company. Penalties may include imprisonment, fines, denial of insurance and civil damages. Any insurance company or agent of an insurance company who knowingly provides false, incomplete, or misleading facts or information to a policyholder or claimant for the purpose of defrauding or attempting to defraud the policyholder or claimant with regard to a settlement or award payable from insurance proceeds shall be reported to the Division of Insurance within the Colorado Department of Regulatory Agencies.

DISTRICT OF COLUMBIA

Warning: It is a crime to provide false or misleading information to an insurer for the purpose of defrauding the insurer or any other person. Penalties include imprisonment and/or fines. In addition, an insurer may deny insurance benefits if false information materially related to a claim was provided by the applicant.

FLORIDA

Any person who knowingly and with intent to injure, defraud, or deceive any insurer files a statement of claim or an application containing any false, incomplete or misleading information is guilty of a felony of the third degree.

KANSAS

A "fraudulent insurance act" means an act committed by any person who, knowingly and with intent to defraud, presents, causes to be presented or prepares with knowledge or belief that it will be presented to or by an insurer, purported insurer, broker or any agent thereof, any written electronic, electronic impulse, facsimile, magnetic, oral, or telephonic communication or statement as part of, or in support of, an application for the issuance of, or the rating of an insurance policy for personal or commercial insurance, or a claim for payment or other benefit pursuant to an insurance policy for commercial or personal insurance which such person knows to contain materially false information concerning any fact material thereto; or conceals, for the purpose of misleading, information concerning any fact material thereto.

KENTUCKY

Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance containing any materially false information, or conceals, for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime.

LOUISIANA

Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

MAINE

It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties may include imprisonment, fines or a denial of insurance benefits.

MARYLAND

Any person who knowingly or willfully presents a false or fraudulent claim for payment of a loss or benefit or who knowingly or willfully presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

NEW JERSEY

Any person who includes any false or misleading information on an application for an insurance policy is subject to criminal and civil penalties.

NEW MEXICO

Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to civil fines and criminal penalties.

NEW YORK

Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information, or conceals for the purpose of misleading, information concerning any fact material thereto, commits a fraudulent insurance act, which is a crime, and shall also be subject to a civil penalty not to exceed five thousand dollars and the stated value of the claim for each such violation.

OHIO

Any person who, with intent to defraud or knowing that he is facilitating a fraud against an insurer, submits an application or files a claim containing a false or deceptive statement is guilty of insurance fraud.

OKLAHOMA

WARNING: Any person who knowingly, and with intent to injure, defraud or deceive any insurer, makes any claim for proceeds of an insurance policy containing any false, incomplete or misleading information is guilty of a felony.

OREGON

Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents materially false information in an application for insurance may be guilty of a crime and may be subject to fines and confinement in prison.

In order for us to deny a claim on the basis of misstatements, misrepresentations, omissions or concealments on your part, we must show that:

A. The misinformation is material to the content of the policy;

B. We relied upon the misinformation; and

C. The information was either:

1. Material to the risk assumed by us; or

2. Provided fraudulently.

For remedies other than the denial of a claim, misstatements, misrepresentations, omissions or concealments on your part must either be fraudulent or material to our interests.

With regard to fire insurance, in order to trigger the right to remedy, material misrepresentations must be willful or intentional.

Misstatements, misrepresentations, omissions or concealments on your part are not fraudulent unless they are made with the intent to knowingly defraud.

PENNSYLVANIA

Any person who knowingly and with intent to defraud any insurance company or other person files an application for insurance or statement of claim containing any materially false information or conceals for the purpose of misleading, information concerning any fact material thereto commits a fraudulent insurance act, which is a crime and subjects such person to criminal and civil penalties.

PUERTO RICO

Any person who knowingly and with the intention of defrauding presents false information in an insurance application, or presents, helps, or causes the presentation of a fraudulent claim for the payment of a loss or any other benefit, or presents more than one claim for the same damage or loss, shall incur a felony and, upon conviction, shall be sanctioned for each violation with the penalty of a fine of not less than five thousand dollars ($5,000) and not more than ten thousand dollars ($10,000), or a fixed term of imprisonment for three (3) years, or both penalties. Should aggravating circumstances be present, the penalty thus established may be increased to a maximum of five (5) years, if extenuating circumstances are present, it may be reduced to a minimum of two (2) years.

RHODE ISLAND

Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.

TENNESSEE

It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

VERMONT

Any person who knowingly presents a false statement in an application for insurance may be guilty of a criminal offense and subject to penalties under state law.

VIRGINIA

It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

WASHINGTON

It is a crime to knowingly provide false, incomplete or misleading information to an insurance company for the purpose of defrauding the company. Penalties include imprisonment, fines and denial of insurance benefits.

WEST VIRGINIA

Any person who knowingly presents a false or fraudulent claim for payment of a loss or benefit or knowingly presents false information in an application for insurance is guilty of a crime and may be subject to fines and confinement in prison.