CYBERCRIME

Businesses and individuals in Alaska increasingly depend on computer networks and electronic data to conduct their daily lives and business operations, growing pools of personal and financial information are being transferred and stored online. When a data breach occurs, this leaves individuals and businesses exposed to privacy violations, and financial institutions and other businesses exposed to potential liability, if and when a data security breach occurs.

Cybercrime and Your Insurance:
As a consumer or business, you may have access to Cyber Insurance in a variety of ways. Some consumers have limited coverage through financial institutions related to loss due to cybercrime/electronic data breach or fraudulent transactions. As a business owner you may have varying levels of coverage under a Commercial Cyber Insurance policy or other Cyber Liability coverage subject to terms and exclusions under your General Liability or Business Owners policy through Electronic Data Liability endorsements or other policy type. Almost all businesses use technology to conduct and transact business thus creating a cyber exposure due to the collection or storage of private data. Cyber Insurance is designed to protect against liability (third-party) and first party claims that occur as a result of damages arising from an insured's cyber exposures. You can find more information about Cybercrime coverage through the resources below and by working with your preferred insurance agent or broker to evaluate your unique business and personal exposures to find a policy that meets your needs.

FIRST STEPS FOR PRODUCERS & INSURERS AFTER DISCOVERY OF CYBERATTACK:

WHEN TO REPORT A CYBER INCIDENT:

If you experience an event that you believe could jeopardize the confidentiality, integrity, or availability of digital information or information systems, report it right away if:

- The event results in a significant loss of data, system availability, or control of systems;
- The event impacts a large number of victims;
- The event indicates unauthorized access to, or malicious software present on critical information technology systems;
- The event affects critical infrastructure or core government functions; or
- The event impacts national security, economic security, or public health and safety

WHAT TO REPORT:

Be prepared to report who you are, who experienced the incident, a description of the incident, an explanation of how and when the incident was initially detected, responses taken, and who has been notified of the incident.

WHERE TO REPORT:

Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to the FBI Field Office Cyber Task Force at http://www.fbi.gov/contact-us/field

Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victims and third parties at **http://www.ic3.gov**
If you have insurance coverage for cybercrime you may contact your insurance carrier at this time.

FIRST STEPS FOR CONSUMERS AFTER NOTIFICATION OF A CYBERATTACK:

In cases of Identity Theft, Financial Fraud, and Hacking;

- Collect and keep evidence including:
  - Canceled checks
  - Certified or other mail receipts
  - Chatroom or newsgroup text
  - Credit card receipts
  - Envelopes (if you received any items)
  - Log all files with date, time and time zone
  - Messages from Facebook, Twitter, and other social media in hard copy, of possible
  - Emails in hard copy, if possible
  - Web pages in hard copy, if possible
  - Money order receipts
  - Pamphlets / brochures
  - Phone bills
  - Wire receipts
- Change password for all online accounts

- Close any unauthorized or compromised credit or charge accounts
- Think about what other personal information might be at risk
- File a report with your local law enforcement agency and/or the Internet Crime Complaint Center www.ic3.gov
- If stolen money or identity is involved, contact one of the three credit bureaus to report the crime
  - Equifax at 1-800-525-6285
  - Experian at 1-888-397-3742
  - TransUnion at 1-800-680-7289
- If you believe someone is using your Social Security Number, contact the Social Security Administration's fraud hotline at 1-800-269-0271

NATIONAL RESOURCES:

- **Internet Crime Complaint Center**

  File complaint online at www.ic3.gov
- **Better Business Bureau**

  Report suspicious email, phone call, website, business practice

  3033 Wilson Blvd, Suite 600
  Arlington, VA 22201
  Phone: (703) 276-0100
- **CyberTipLine**

  Investigates cases of online sexual exploitation of children

  699 Prince Street
  Alexandria, VA 22314-3175
  Phone (703) 224-2150
  Fax (703) 224-2122
- **StopFraud.gov**

  Victims of fraud resources & fraud reporting

  Phone: (202) 514-2000

  Email: ffetf@usdoj.gov

- **US Department of Justice: Computer Crime Section**

  10th & Constitution Ave., NW
  John C. Keeney Building, Suite 600
  Washington, DC 20530
  Phone: (202) 514-1026
  Fax: (202) 514-6113

ADDITIONAL LINKS AND RESOURCES:

https://www.justice.gov/criminal-ccips/file/1096971/download

https://www.usa.gov/online-safety