NAIC Roadmap for Cybersecurity Consumer Protections

This document describes the protections the NAIC believes consumers are entitled to from insurance companies, agents and other businesses when they collect, maintain and use your personal information, including what should happen in connection with a notice that your personal information has been involved in a data breach. Not all of these consumer protections are currently provided for under state law. This document functions as a Consumer Bill of Rights and will be incorporated into NAIC model laws and regulations. If you have questions about data security, a notice you receive about a data breach or other issues concerning your personal information in an insurance transaction, you should contact your state insurance department to determine your existing rights.

As an insurance consumer, you have the right to:

1. Know the types of personal information collected and stored by your insurance company, agent or any business it contracts with (such as marketers and data warehouses).
2. Expect insurance companies/agencies to have a privacy policy posted on their websites and available in hard copy, if you ask. The privacy policy should explain what personal information they collect, what choices consumers have about their data, how consumers can see and change/correct their data if needed, how the data is stored/protected, and what consumers can do if the company/agency does not follow its privacy policy.
3. Expect your insurance company, agent or any business it contracts with to take reasonable steps to keep unauthorized persons from seeing, stealing or using your personal information.
4. Get a notice from your insurance company, agent or any business it contracts with if an unauthorized person has (or it seems likely he or she has) seen, stolen or used your personal information. This is called a *data breach*. This notice should:
   - Be sent in writing by first-class mail or by e-mail if you have agreed to that.
   - Be sent soon after a data breach and never more than 60 days after a data breach is discovered.
   - Describe the type of information involved in a data breach and the steps you can take to protect yourself from identity theft or fraud.
   - Describe the action(s) the insurance company, agent or business it contracts with has taken to keep your personal information safe.
   - Include contact information for the three nationwide credit bureaus.
   - Include contact information for the company or agent involved in a data breach.
5. Get at least one year of identity theft protection paid for by the company or agent involved in a data breach.
6. If someone steals your identity, you have a right to:
   - Put a 90-day initial fraud alert on your credit reports. (The first credit bureau you contact will alert the other two.)
   - Put a seven-year extended fraud alert on your credit reports.
   - Put a credit freeze on your credit report.
   - Get a free copy of your credit report from each credit bureau.
   - Get fraudulent information related to the data breach removed (or "blocked") from your credit reports.
   - Dispute fraudulent or wrong information on your credit reports.
   - Stop creditors and debt collectors from reporting fraudulent accounts related to the data breach.
   - Get copies of documents related to the identity theft.
   - Stop a debt collector from contacting you.

To learn more about the protections in your state or territory, contact your consumer protection office at *https://www.usa.gov/state-consumer* or your state or territory's insurance department at *www.naic.org/state_web_map.htm*.

Standard Definitions Under This Bill of Rights

Data Breach: When an unauthorized individual or organization sees, steals or uses sensitive, protected or confidential information—usually personal, financial and/or health information.

Credit Bureau (Consumer Reporting Agency): A business that prepares credit reports for a fee and provides those reports to consumers and businesses; its information sources are primarily other businesses.

Credit Freeze (Security Freeze): A way you can restrict access to your credit report and prevent anyone other than you from using your credit information.

Personal Information (Personally Identifiable Information): Any information about a consumer that an insurance company, its agents or any business it contracts with maintains that can be used to identify a consumer. Examples include:

- Full name.
- Social Security number.
- Date and place of birth.
- Mother's maiden name.
- Biometric records.
- Driver's license number.

Helpful Links:

"Credit Freeze FAQs" (Federal Trade Commission—FTC) – *www.consumer.ftc.gov/articles/0497-credit-freeze-faqs*

"Disputing Errors on Credit Reports" (FTC) – *www.consumer.ftc.gov/articles/0151-disputing-errors-credit-reports*

"Taking Charge: What to Do If Your Identity Is Stolen" (FTC, May 2012). Tri-fold brochure; online PDF; can order bulk copies at no cost – *https://bulkorder.ftc.gov/system/files/publications/pdf-0009-taking-charge.pdf*

"Know Your Rights" (FTC) – *https://www.identitytheft.gov/know-your-rights.html*

"What Is Identity Theft?" (video; FTC) – *www.consumer.ftc.gov/media/video-0023-what-identity-theft*

"When Information Is Lost or Exposed" (FTC) – *https://www.identitytheft.gov/info-lost-or-stolen.html*

State Consumer Protection Offices (USA.gov) – *www.usa.gov/directory/stateconsumer/index.shtml*

Directory of State Insurance Regulators (NAIC) *www.naic.org/state_web_map.htm*

World's Biggest Data Breaches (information is beautiful) – *www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/*