Hack-E-Sacked:
Consumer Perspectives on Insurance Cybersecurity

Presentation to
Insurance Regulatory Examiners Society
Career Development Seminar

Birny Birnbaum
Center for Economic Justice

July 21, 2015

The Center for Economic Justice

CEJ is a non-profit consumer advocacy organization dedicated to representing the interests of low-income and minority consumers as a class on economic justice issues. Most of our work is before administrative agencies on insurance, financial services and utility issues.

On the Web: www.cej-online.org

Why CEJ Works on Insurance Issues

Essential Financial Security Tool for Individual and Community Economic Development: CEJ Works to Ensure Access and Fair Prices for These Essential Products and Services, particularly for Low- and Moderate-Income Consumers.

Primary Institution to Promote Loss Prevention and Mitigation: CEJ Works to Ensure Insurance Institutions Maximize Their Role in Efforts to Reduce Loss of Life and Property from Catastrophic Events.

Topics

1. Why are Insurers a Growing Target for Hacking?
2. What Should an Insurance Consumer Cybersecurity Bill of Rights Include?
3. What Are the Opportunities for Insurers to Grow the Cyberinsurance Market?

Why are Insurers a Growing Target for Cyber Thieves?

Insurers have always been in the data collection and data management business, but historically the data collected was limited. Consider data collected by auto and home insurers as recently as 20 years ago – information on a relatively few rating characteristics. Now consider how that has changed as insurers started utilizing credit information (and collecting Social Security Numbers) and data mining non-insurance data (web browsing, shopping and other info compiled by data brokers, Google, Apple) and new categories of insurance data (more granular claims data, telematics; drones).

Simply stated, insurers are where the money is.

Proposed Insurance Consumer Cybersecurity Bill of Rights

1. Transparency of Information Collected and Maintained: ***Consumers Have the Right to Know What Personal Information is Collected, How Long the Personal Information is Maintained and To Require Destruction of Non-Essential Data.***

a. Disclosure to Consumers of Information Collected, How Long Information Is Kept, Security Measures to Protect Stored Information, and Intended Use.

b. Requirement for Insurers to Obtain Opt In to Collect and/or Store Personally-Identifying Information Not Essential for Insurance Purposes. One example of such non-essential information for some types of insurance is Social Security Number.

c. Consumers' Opportunity to Correct Erroneous Information

Proposed Insurance Consumer Cybersecurity Bill of Rights

2. Strong, Minimum Standards for Data Protection: ***Consumers Have the Right to Adequate and Reasonable Safeguards of Personal Information by the Insurer.***

   a. Regulatory Oversight of Data Security with Clear and Severe Penalties for Inadequate Data Security. Regulators would not let an insurer operate if it could not account for and protect money given by a consumer to the insurer; data provided to insurers are as valuable if not more so and should be protected as such.

Proposed Insurance Consumer Cybersecurity Bill of Rights

3. Prompt and Full Disclosure of Data Theft—***Consumers Have the Right to Be Fully and Promptly Informed If Personal Information Is Stolen or Lost.***

a. Disclosure to consumers of information stolen and when stolen to enable consumers to take necessary and timely actions to protect themselves.

Proposed Insurance Consumer Cybersecurity Bill of Rights

4. Assistance to Consumers to Deal with Data Breach – ***Consumers Have the Right to Assistance and Restitution from an Insurer Who Fails to Protect Personal Information.***

   a. Type and Duration of Assistance will vary by type of data stolen – credit card numbers vs. SSN; E-mail address vs. medical history.

Proposed Insurance Consumer Cybersecurity Bill of Rights

5. Regulatory Oversight of Personal Cyberinsurance – ***Consumers Have the Right to Meaningful Benefits from Personal Cyberinsurance Policies.***

   a. Regulators must fully enforce laws requiring that such insurance should not be misleading or deceptive or that such insurance should provide more than illusory coverage.

   b. In an emerging market, regulatory guidance is critical. Broad regulatory guidance to ensure that new personal cyberinsurance products have real value, are not misleading and provide more than illusory coverage is especially important at the dawn of this new era of cyberinsurance. Such broad regulatory guidance is consistent with promotion of competitive markets and consumer protection.

Emerging Cyber Risks Create a Market for Insurers to Demonstrate the Key Role of Insurers and Insurance in Loss Mitigation

Insurers have had a strong history of leading the way on loss mitigation, from fire safety to engineering boiler safety.

There is a great opportunity for insurers to develop cyberinsurance products that are primarily loss mitigation assistance to policyholders with coverage for residual risk, in the same way that, for example, Hartford Steam Boiler, is primarily in the loss mitigation business with residual insurance coverage.

The loss mitigation potential is great by raising awareness and understanding of basic data security measures.