

WEEK OF
December 2nd
2013



Days until
the **#MandateTax**
takes effect:

119

Key Message Themes

“Obamacare Increases Health Care Costs”

“Because of Obamacare, I Lost My Insurance”

“The Exchanges May Not Be Secure, Putting Personal Information at Risk”

Action Items

Use Social Media and Other Resources to Make Sure Your Constituents are Aware of the Obamacare Scams and the Security Risks.

Hearings

“The Roll Out of HealthCare.gov: The Limitations of Big Government.” Hearing 12/4.

Oversight & Government Reform

“Medicare Advantage: What Beneficiaries Should Expect Under the President’s Health Care Plan.” Hearing 12/4.

Energy & Commerce (Health)

“The Health Care Law: The Effect of the Business Aggregation Rules on Small Employers.” Hearing 12/4.

Small Business

Obamacare implementation: immediate and long-term challenges. Hearing 12/4.

Ways & Means (Health)

“Obamacare Implementation, The Broken Promise: If You Like Your Current Plan You Can Keep It.” Field Hearing, Apache Junction, AZ, 12/6.

Oversight & Government Reform

Examples of Obamacare Security Concerns:

Morgan Wright, Chief Executive Officer, Crowd Sourced Investigations, LLC:

"It's not secure. We would not put our family on it. We wouldn't tell anybody to get on it; not at this time, not in the near future."

Matthew J. Belvedere, "[Fix Obamacare site? 'Better chance of seeing God'.](#)" *CNBC*, Nov. 21, 2013.

From Wright's testimony at Science Committee Hearing:

"The site lacks both the proper security controls and comprehensive security test plan... it also creates massive opportunity for fraud, scams, deceptive trade practices, identity theft and more."

David Kennedy, Chief Executive Officer, Trusted SEC, LLC:

"If a hacker wanted access to the site or sensitive information – they could get it," he told FoxNews.com.

"[Healthcare.gov 'may already have been compromised,' security expert says.](#)" *FoxNews.com*, Nov. 19, 2013.

Former Social Security Administrator (retired last year), Michael Astrue:

"It's a hacker's dream."

Michael Isikoff, "[Sebelius defends Obamacare site's security, but questions mount.](#)" *NBC News*, Oct. 30, 2013.

Georgetown Professor, who is a supporter of Obamacare, but critical of its security:

"Nothing can undermine public confidence more than the fear of a security and privacy breach," Gostin said. "You could have somebody hack into the system, get your Social Security number, get your financial information."

Sharyl Attkisson, "[HealthCare.gov ducked final security requirements before launch.](#)" *CBS News*, Nov. 4, 2013.

Attorney General Greg Abbott of Texas:

"The flaws could allow criminals to obtain Texans' personal financial and health information through navigator sloppiness, Abbott warned."

Robert Garrett, "[Abbott Suggests State Will Boost Requirements on Obamacare Navigators.](#)" *Dallas Morning News*, Nov. 25, 2013.

Letter from 10 Attorneys General:

"Perhaps most troubling are outstanding security concerns related to the ACA's technology and outreach personnel... For example, after logging on to the federal exchange website, a North Carolina resident was granted access to the downloadable eligibility letter that contained the personal information of two individuals from South Carolina."

Letter from Attorney General Patrick Morrisey et al. to Secretary Kathleen Sebelius, "A communication from the States of WV, AL, FL, GA, KS, LA, OK, SC, TX, and UT regarding the readiness of the new health insurance exchanges," Nov. 6, 2013.

Letter from Identity Theft Resource Center:

"Our first and foremost concern is the lack of a federal requirement to conduct background checks on the program navigators... Our other main concern is that healthcare.gov website requires a visitor to divulge their personal information before they are allowed to peruse the website and shop for Health coverage."

Letter from Eva Velasquez to Chairman Lamar Smith, Nov. 15, 2013.

Mother Jones Article:

"Common clickjacking would be a popular method to attempt to exploit [the site]" says Wilhoit. "Hackers could use this information in the creation of fake identities, fake credit cards, and fake accounts very easily."

Dana Liebelson, "[How Healthcare.gov Could be Hacked.](#)" *Mother Jones*, October 24, 2013.

Examples of Documented Obamacare Scams:

"It's an opportunity for scammers, and scammers very rarely leave an opportunity unfulfilled," said Mark Rasch, a former computer crime and fraud prosecutor with the U.S. Department of Justice.

<http://www.usatoday.com/story/news/nation/2013/11/11/affordable-care-act-scams/3501595/>

Obamacare scams come in a variety of forms. Consumers have complained about con artists contacting them by phone, fax, email and even in person.

<http://www.fraud.org/component/content/article/2-uncategorised/60-bogus-magazine-2>

A common version of the scam involve fraudsters claiming to be from the federal government and directing consumers to purchase insurance cards in order to be eligible for coverage under the ACA. Scammers intimidate consumers to give them their bank account routing numbers or make a direct cash transfer by using words like "it is the law" or "the government now requires it."

<http://www.fraud.org/component/content/article/2-uncategorised/60-bogus-magazine-2>

In **Massachusetts**, scammers deceptively marketed fake health insurances policies and created fake Web sites that claimed to sell Obamacare, targeting seniors to gain their personal information.

<http://www.fraud.org/component/content/article/2-uncategorised/60-bogus-magazine-2>

In other cases in **Kansas** and **Alabama**, con artists posing as government employees conned consumers into divulging their bank account numbers in order to sign up for fake health care plans. Fraudulent health insurance plans are being offered by these criminals for as little as \$29.95 per month.

<http://www.fraud.org/component/content/article/2-uncategorised/60-bogus-magazine-2>

An advertising company in **Nevada** reported to have received faxes from no-name companies that claimed to provide insurance at \$29.99.

<http://www.fraud.org/component/content/article/2-uncategorised/60-bogus-magazine-2>

According to a *Houston Chronicle* report, scammers have threatened consumers with jail time if they don't purchase the fake insurance cards.

<http://www.fraud.org/component/content/article/2-uncategorised/60-bogus-magazine-2>

Scammers claiming to be navigators or Medicare officials, trick seniors and low-income consumers into divulging personal information and paying for fictitious insurance plans.

<http://www.fraud.org/component/content/article/2-uncategorised/60-bogus-magazine-2>

The Better Business Bureau reported that a company in **Arizona** deceived a senior into providing her bank account number by claiming that she was qualified to sign up for Obamacare, and that there were only twenty spots left.

Fraudsters have also frequently directed consumers to wire money or send funds via a prepaid card if they want the full benefits of Obamacare. In the month of May alone, the Federal Trade Commission received over 1,100 complaints about similar scams.

<http://www.fraud.org/component/content/article/2-uncategorised/60-bogus-magazine-2>

Ohio's Department of Insurance issued a warning with the state Attorney General's Office just days after ACA enrollment officially opened last month that the scam gates had opened. Ohio Attorney General Mike DeWine and Insurance Director and Lieutenant Gov. Mary Taylor warned that scammers were pretending to be associated with the government to make the ploys believable.

<http://www.usatoday.com/story/news/nation/2013/11/11/affordable-care-act-scams/3501595/>

According to a press release from **California** Attorney General Kamala D. Harris, her state has closed down at least 10 websites set up to take advantage of applicants, and Time magazine reported that **Kentucky** and **Pennsylvania** have also had to deal with scam sites.

<http://www.ibtimes.com/obamacare-fallout-whats-worse-broken-healthcare-website-california-shuts-scam-websites-1472060>