



Online Trust Audit Briefing June 14, 2016

UNDERWRITERS



LEARN • INNOVATE • COLLABORATE



Craig Spieze
Executive Director & President

Jeff Wilbur
VP, Industry Insights & Research



LEARN • INNOVATE • COLLABORATE

Online Trust Audit & Honor Roll

Objectives:

- Move from a “compliance” mindset to “stewardship”
- Drive adoption of best practices
- Recognize excellence in consumer protection, data security and *responsible* privacy practices.
- Increase consumer awareness of sites who demonstrate commitment to security and privacy principles.

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 3



LEARN • INNOVATE • COLLABORATE

Disclaimer

- Audit was conducted April 15 – May 15
- There is no perfect security or privacy.
- “Snap Shot”, sites and data may have changed.
- Does not reflect an audit of business practices.
- Is not an endorsement of any company or service.
- Several sites advised OTA of updates. Where validated they were re-scored, impacting ranking.

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 4



LEARN • INNOVATE • COLLABORATE

Congressional Views



© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 5

OTA
Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Making Security & Privacy Count



- **David C. Vladeck**, Professor, Georgetown Law School
- **William Carty**, Manager Public Policy, Twitter
- **Kim Meehan**, SVP Operations, LivingSocial
- **Gary VonHoch**, VP Web Operations, AG Interactive
- **Melanie Wyne**, National Association of REALTORS

© 2016 All rights reserved. Online Trust Alliance (OTA)

Slide 6

OTA
Online Trust Alliance

LEARN • INNOVATE • COLLABORATE

Honor Roll Overview

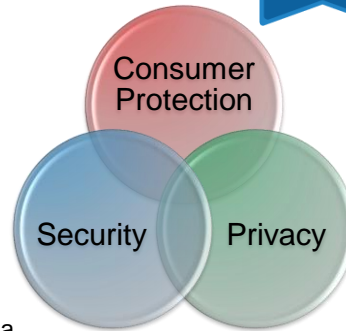


- **Audit of 1,000 web sites**

- Internet Retailer Top 500
- FDIC Banking 100
- Top 100 Consumer Services
- Top 100 News/Media
- Top 50 Federal Gov't
- OTA Members

- **Scoring**

- 100 baseline points for each category
- Weighted composite analysis, ~50 criteria
- Bonus points for emerging practices
- Penalty points for
 - Vulnerabilities, privacy practices, data loss incident & fines/settlement
- Honor Roll = 80% of total points, 55% or better in each category



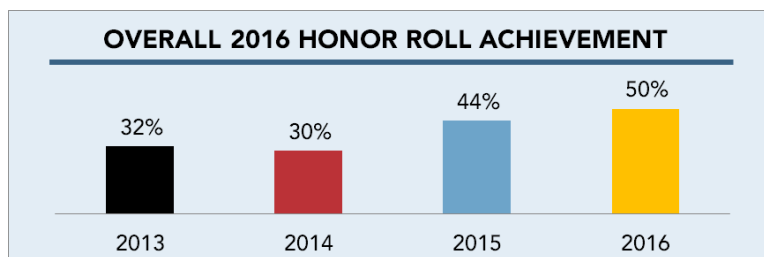
© 2016. All rights reserved. Online Trust Alliance (OTA)

Slide 7



LEARN • INNOVATE • COLLABORATE

Honor Roll Recap



- Record achievement despite a bar that continues to rise
- 183 “first-timers” (~40%)
- 54 qualified for 5 consecutive years (~12%)
- Range of retailers #1 to #493, showing bar is achievable

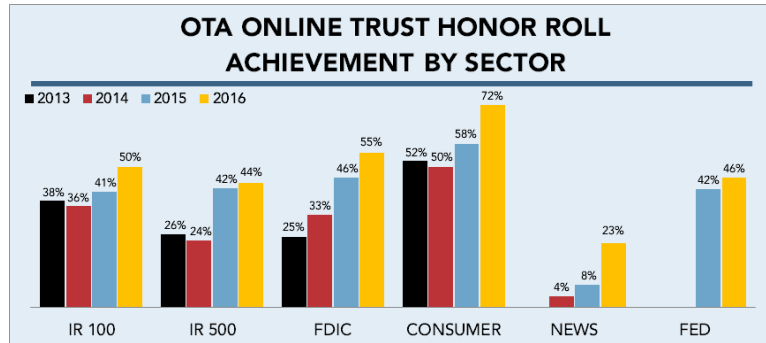
© 2016. All rights reserved. Online Trust Alliance (OTA)

Slide 8



LEARN • INNOVATE • COLLABORATE

Growth in All Sectors

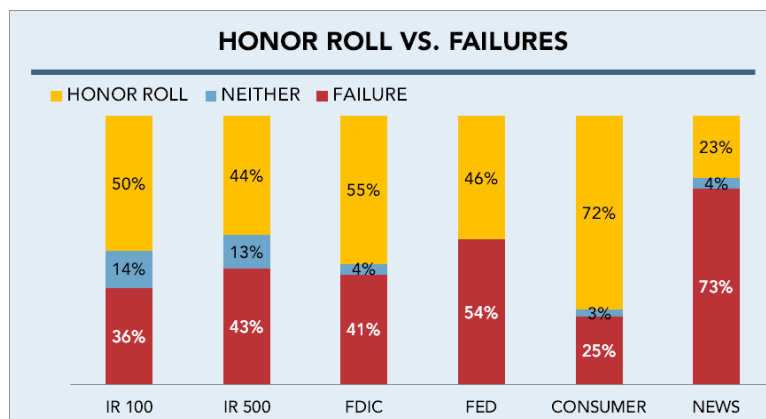


- Nearly 3-fold increase in News, yet they still lag all sectors, primarily due to data sharing with limited controls



LEARN • INNOVATE • COLLABORATE

Failing vs Stewardship

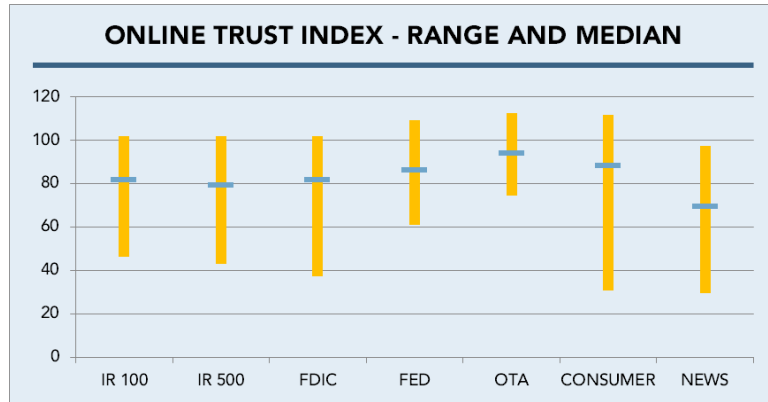


- 4 categories bi-modal (or nearly)



LEARN • INNOVATE • COLLABORATE

Range & Median

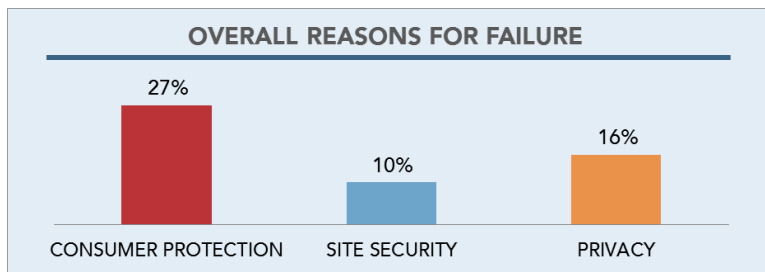


- Retailers and FDIC banks median is at 80% Honor Roll bar
- Consumer and Fed sites outperform, while News lags



LEARN • INNOVATE • COLLABORATE

Summary of Failures

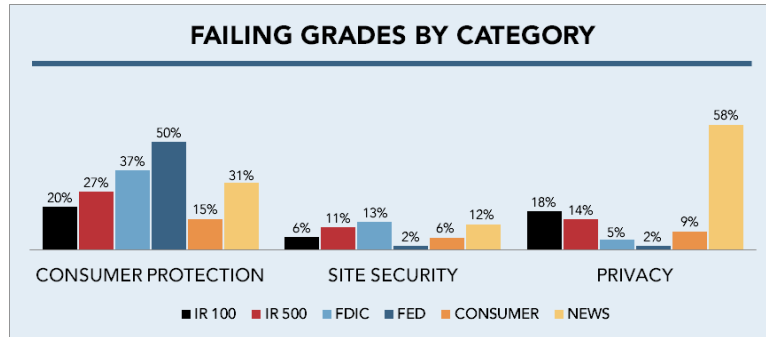


- Sites can fail in multiple categories



LEARN • INNOVATE • COLLABORATE

Primary Areas of Concern

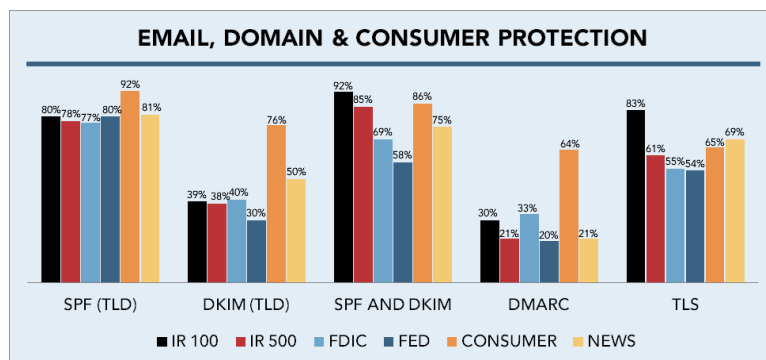


- Addressable deficiencies in consumer protection independent of business practices or models
- Privacy impacted by business practices and lack of clarity in privacy policies



LEARN • INNOVATE • COLLABORATE

Consumer Protection

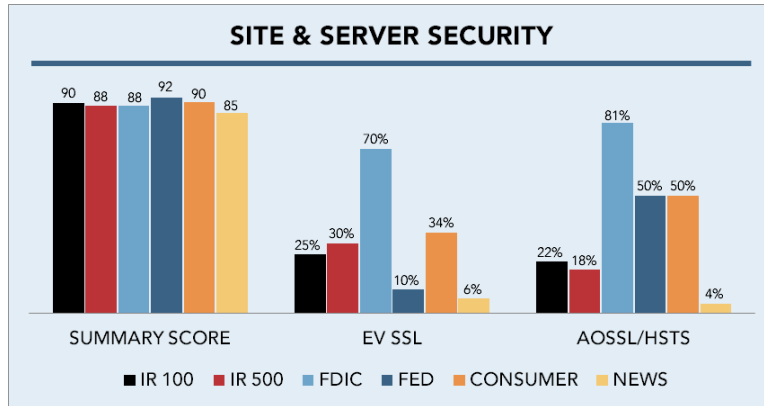


- Aids in protection from social engineering exploits including spearphishing & ransomware



LEARN • INNOVATE • COLLABORATE

Site & Data Security

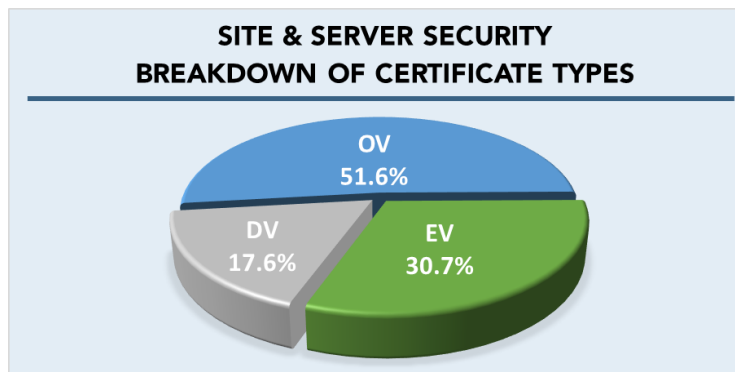


- Overall average scores tightly clustered, yet a wide range of adoption of key standards advocated by the FDIC, IRS, OMB and industry



LEARN • INNOVATE • COLLABORATE

Concerns – Certificate Type

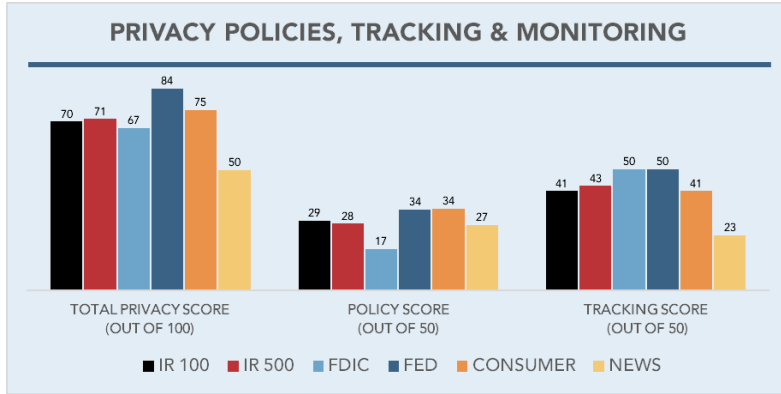


- Recommend OV or EV for increased trust/transparency.
- Rise in fraudulent/lookalike sites that typically use DV certs.



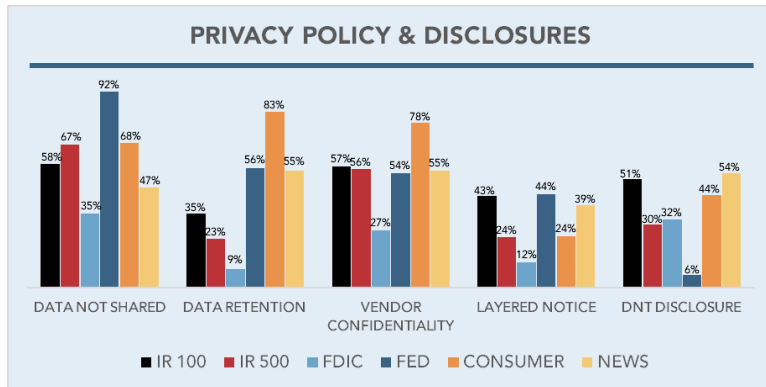
LEARN • INNOVATE • COLLABORATE

Privacy – Missing Link



LEARN • INNOVATE • COLLABORATE

Privacy – Missed Opportunities



- 1.3% include icons, 4.5% localize their policy
- 73.7% date stamp, yet only 4.1% post older revisions



LEARN • INNOVATE • COLLABORATE

General Observations

- Lack of continuous monitoring of site / server configurations
- Attempts to contact sites with vulnerabilities failed due to lack of vulnerability reporting mechanism and not monitoring their domain technical contact.
- Privacy policies still exhibit poor readability and excessive language that is not user friendly.
- High levels of data collection and sharing via use of tracking tags, ranging from 0 to 125 per site.
- Failures due to lack of email authentication put consumers at unnecessary levels of risk.



LEARN • INNOVATE • COLLABORATE

Attendees Honor Roll

*Recognizing Excellence in Consumer Protection,
Security & Responsible Privacy Practices*



LEARN • INNOVATE • COLLABORATE

2016 Top Ten



1. Twitter (twitter.com)
2. HealthCare.gov (healthcare.gov)
3. Pinterest (pinterest.com)
4. The White House (whitehouse.gov)
5. Dropbox (dropbox.com)
6. FileYourTaxes (fileyourtaxes.com)
7. LifeLock (lifelock.com)
8. Instagram (instagram.com)
9. 1040.com(1040.com)
10. Gap Inc. (gap.com)



LEARN • INNOVATE • COLLABORATE

Open Dialog - Questions

- Webinar June 28th
<https://attendee.gotowebinar.com/rt/2197260013273562371>
- Input into 2017 methodology and scoring
 - Open Call for comments
 - Increased focus on privacy disclosures
 - Deeper security assessments including open ports / relays
 - Adoption of multi-factor authentication
- New sectors under consideration / pending funding
 - ISPs, Cable Providers and Carriers
 - 50 States, focused on TBD core consumer agency(s)
 - State e-file sites
 - IoT devices & services



LEARN • INNOVATE • COLLABORATE



Thank You



UNDERWRITERS



LEARN • INNOVATE • COLLABORATE