7th Annual Online Trust Audit

Honor Roll Highlights – Leading Web Merchants

Released June 3, 2015

OVERVIEW

Now in its seventh year, the OTA Online Trust Audit has become the benchmark independent audit of businesses' commitment to security, privacy and consumer protection.[1] The audit evaluates over three-dozen data attributes incorporated into a composite weighted analysis of broadly accepted best practices. This special report is based on the rankings compiled in Internet Retailer's 2015 edition of The Top 500,[2] and segments the Internet Retailer Top 100 from the Internet Retailer Top 500 for comparison purposes. The comprehensive audit is a subset of the 2015 Online Trust Audit of nearly 1,000 sites – including banking, social, Internet of Things (IoT), media / content sites and top U.S. government agencies – which will be released in mid-June.

Consistent with the goals of the Online Trust Alliance, a 501c3 non-profit organization, the goal of the audit is to promote and accelerate the adoption of consumer protection-enhancing best practices, recognize leadership, data stewardship and commitment to meaningful self-regulation.

This audit serves as the foundation for business and technical decision makers as they bring new products and services to the market. As the cyber threat increases and privacy concerns heighten, the relevancy and timeliness of this report is significant, underscoring the imperative that data security, protection and privacy need to be integrated into every service, business process, web site and mobile application.

The 2015 methodology reflects input and review through a multi-stakeholder process, evaluating current standards, best practices and leading causes of data breach incidents. Feedback and recommendations incorporated into the methodology publicly released in March included additional data attributes, enhanced granularity to site security and privacy practices, increased weighting in several core areas and shifting of some 2014 bonus points to baseline scoring.

By design the report is designed to recognize leadership while promoting the critical importance for organizations of all sizes to adopt consumer centric best practices. Organizations that have followed suit are to be commended for their commitment to their customers.

---

[1] Online Trust Audit & Honor Roll https://otalliance.org/HonorRoll

[2] Internet Retailer and Vertical Web Media http://www.top500guide.com/about/. The Top 500 ranks the 500 largest e-retailers in North America based on annual web sales.

Based on the composite weighted analysis, **2015's top 10 most trustworthy online retailers** (technically 11 due to a tie) include:

- American Greetings
- Cabela's
- Drs. Foster & Smith
- Fanatics
- GameStop
- The Honest Company
- Jomashop
- Kate Spade New York
- LivingSocial
- Netflix
- SparkFun Electronics

In light of the number of high profile data breaches over the past 24 months, the authors of this report considered automatically disqualifying a retailer if they experienced a data breach. However, recognizing there is no perfect security and the desire to not dissuade companies from public disclosure of such incidents, in the 2015 methodology the negative scoring for a breach was instead increased by three-fold, a stiff penalty that nevertheless could still be overcome. It should be noted some retailers who experienced a breach incident had top scores in every category and subsequently qualified for the Honor Roll.

It is important to recognize that this analysis is limited to a slice of time. Readers should look at retailers who have consistently made the Honor Roll as well as those that have been conspicuously absent year after year. Retailers who have failed to adopt a security and privacy by design culture and a data stewardship mindset risk disenfranchising consumers, and may validate the need for increased regulatory oversight while inviting lawsuits from consumers and stockholders.

HIGHLIGHTS

- 42.4% of the largest online retailers in North America qualified, up from 24% in 2014. This is a testimony to making an investment in consumer protection, security and privacy best practices.
- Qualifying for the Honor Roll is achievable by companies of all sizes ranging from Amazon ranked #1 with online revenues estimated at $79 billion and Sketchers ranked #499 with estimated revenues of $27 million.[3, 4]
- The 2015 methodology and scoring criteria in all areas were raised and tightened to reflect the increased sophistication of cybercrime activities, threat landscape and documented vulnerabilities and the need to move towards consumer-centric privacy practices.[5]
- Small changes in one or two of the scored criteria allowed nearly 100 additional retailers to make the Honor Roll in 2015. In 2014, they were within 6% (15 points) of qualifying.
- The gap between the Internet Retailer Top 100 and Internet Retailer Top 500 narrowed in all categories with the exception of email authentication.[6, 7]

[3] http://www.marketwatch.com/investing/stock/amzn/financials
[4] http://skx.com/investor/
[5] https://otalliance.org/initiatives/2015-honor-roll-methodology
[6] https://otalliance.org/eauth
[7] Note for illustration purposes the Internet Retailer Top 100 is referred to as the "IR 100" and the Internet Retailer Top 500 is referred to as the "IR 500"

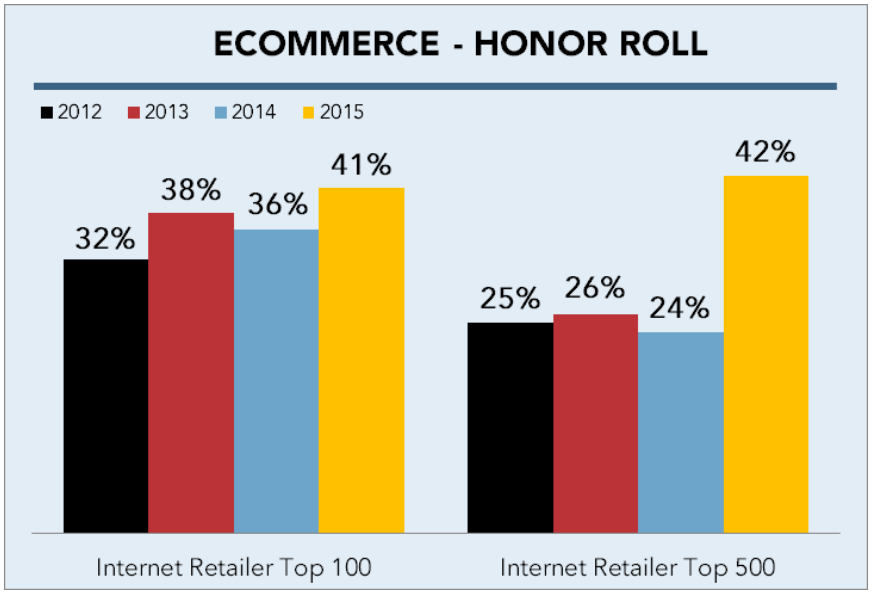

Figure 1 - Honor Roll Trends

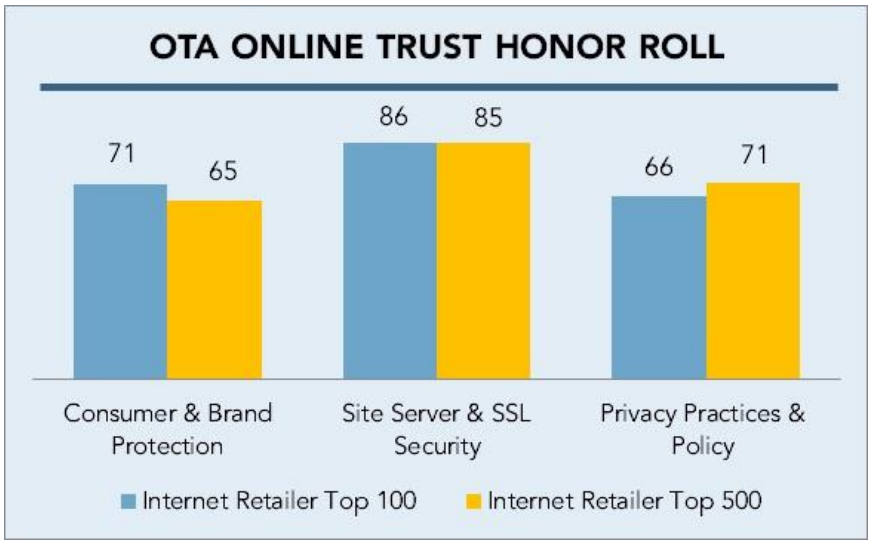

Figure 2- Average sector scores, out of 100 base points

eCOMMERCE KEY METRICS				
	2012	2013	2014	2015
Honor Roll	25.0%	25.6%	23.8%	42.4%
Email Authentication (Any)	90.6%	88.0%	98.0%	94.6%
Any SPF	62.5%	78.6%	91.0%	89.2%
Any DKIM	69.5%	65.0%	81.2%	83.0%
Email Authentication (Both)	43.0%	55.6%	74.2%	77.6%
Site Security Average	76.8	85.1	83.3	85.3
EVSSL	30.7%	33.4%	35.0%	32.1%
Privacy Score (Average)	63.5	64.4	63.6	71.0

Figure 3 - Top Level Trends

TOP 10 RETAILERS

- American Greetings, Cabela's, Drs. Foster and Smith, Fanatics, GameStop, Honest Company, Jomashop, Kate Spade, LivingSocial, Netflix and SparkFun Electronics, (11 due to a scoring tie).
- For the third year, American Greetings achieved the highest score among all retailers.
- The top ten ranged from #6 ranked Netflix to SparkFun Electronics at #463.
- Of the top 10 retailers, 2 repeated from 2014 (American Greetings and Netflix).
- 5 of the top 10 are first time recipients of the Honor Roll.

FAILURES

- 45% failed in one or more categories, leaving 13% of sites who neither failed nor qualified for the Honor Roll. Compared to 2014, failures within categories declined –
    - 22% failed due to inadequate domain / consumer protection from spoofed and malicious email (down from 26% in 2014).
    - 27% failed due to inadequate privacy policies, failure to provide disclosure and/or overly aggressive data collection with third parties without controls (down from 34% in 2014).
    - 5% failed due to server security issues (down from 11% in 2014), reflecting that sites have increased operational focus to address known vulnerabilities and best practices.
- **Data Breaches** – The penalty for a data breach was tripled, representing the severity of data breaches and impact to identity theft. Recognizing there is no perfect security, a disclosed data breach did not result in automatic disqualification.

CONCERNS & RECOMMENDATIONS

- Adoption of email authentication at the top-level domain, which is often spoofed, remained flat at 27%, putting consumers at a heightened risk of spear phishing and related exploits.
- DMARC adoption remains disappointingly low at only 8.2%. Sites need to migrate to DMARC reject policies to optimize protection from malicious email. Only 1% of the top retailers have such policies and only 14.6% of those with DMARC polices published such actionable policies to reject or quarantine malicious or forged email.[8]
- Internet retailers' privacy policies lack basic disclosures and/or are not optimized for consumer readability. OTA advocates for short layered privacy policies and clearly defined data collection, retention and sharing practices. Lack of Do Not Track (DNT) disclosure is concerning as over 75% of sites are failing to comply with California disclosure notice requirements.
- Disappointingly, only 13% of retailers have embraced "Always On SSL" (AOSSL). Sites are encouraged to implement AOSSL not only to increase consumer data protection, but also to realize optimized search engine results by Google and others.[9] [10]
- Though overall improvement was seen, key security fundamentals remain overlooked – 23% remain vulnerable to BEAST, 20% remain vulnerable to Heart Bleed and less than 40% have web application firewalls. 28% have yet to upgrade to SHA2 certificates and 23% failed to address RC4 issues.

[8] https://otalliance.org/DMARC
[9] https://otalliance.org/AOSSL
[10] http://googlewebmastercentral.blogspot.com/2014/08/https-as-ranking-signal.html

2015 eCOMMERCE ONLINE TRUST HONOR ROLL RECIPIENTS

1-800 Contacts Inc.
AAFES
AC Lens
Adobe Systems Inc.
2 AJ Madison Inc.
4 Alibris Inc.
2 Allied Electronics
4 Amazon.com Inc.
American Girl LLC
4 **American Greetings Corp.**
AmeriMark Direct LLC
Amway
4 Ancestry.com Inc.
APMEX Inc.
ASOS.com Ltd.
AutoZone Inc.
Avon Products Inc.
BabyAge.com Inc.
Balsam Brands
2 Bare Escentuals Inc.
BarnesandNoble.com
BCBG Max Azria Group LLC
Beachbody LLC
bebe stores Inc.
3 Bellacor Inc.
3 Best Buy Co. Inc.
4 Big Fish Games Inc.
4 BikeBandit.com
BJ's Wholesale Club
Boden USA
Bonobos
Brooks Brothers
3 Build.com Inc.
3 BuildASign.com
BuildDirect Technologies Inc.
Burberry Ltd.
4 **Cabela's Inc.**
Charlotte Russe Inc.
Chegg Inc.
2 Christianbook.com LLC
Coach Inc.
2 Coastal Contacts Inc.
Colony Brands Inc.
Columbia Sportswear Co.
Costco Wholesale Corp.
CPO Commerce LLC
Crutchfield Corp.
4 CustomInk
Destination XL Group Inc.
Diamond Nexus
2 Dillard's Inc.
Discount Dance Supply
3 DiscountRamps.com LLC
3 Disney Store USA LLC
Dollar Shave Club
2 DoMyOwnPestControl.com
Drs. Foster and Smith
DSW Inc.
eBags Inc.
Eddie Bauer LLC
Edible Arrangements
Entertainment Earth Inc.
eSalon
Estee Lauder
3 Etsy Inc.
3 evo
2 Express Inc.
Fanatics Inc.
4 Fathead LLC
Forever 21
Fossil Inc.
FreshDirect LLC
3 GameFly Inc.
4 **GameStop Corp.**
Gap Inc.
Gilt Groupe
Golfsmith International
Hallmark Cards Inc.
Hammacher Schlemmer
Hanna Andersson Corp.
4 Hayneedle Inc.
Hot Topic Inc.
4 HSN Inc.
3 Hulu LLC
3 Ice.com
2 ID Wholesaler
iHerb Inc.
IKEA.com
3 JackThreads.com
Jenson USA
JimmyJazz.com
Joann.com
Jomashop.com
K&L Wine Merchants
3 Karmaloop.com
Kate Spade
Keurig Green Mountain Inc.
Lamps Plus Inc.
LD Products
LifeWay Christian Resources
3 **LivingSocial Inc.**
Luxottica Group S.p.A.
Macy's Inc.
Mason Companies Inc.
MEC
4 Microsoft Corp.
3 Minted
4 ModCloth Inc.
Monoprice Inc.
Musician's Friend Inc.
NAPA
National Builder Supply
National Football League
National Hockey League
NBTY Inc.
2 Nebraska Furniture Mart
Neebo Inc.
4 **Netflix Inc.**
3 New Balance
2 Newegg Inc.
2 Nike Inc.
Nine West Holdings Inc.
2 Nordstrom Inc.

2015 eCOMMERCE ONLINE TRUST HONOR ROLL RECIPIENTS (Cont)

Northern Tool & Equipment
Nuts.com
OmahaSteaks.com Inc.
Online Stores Inc.
OpticsPlanet Inc.
Orchard Brands Corp.
❷ OvernightPrints.com
❹ Overstock.com Inc.
❸ Pacific Sunwear
Pandora
Parts Express
Party City Corp.
❹ Payless ShoeSource Inc.
❹ PersonalizationMall.com
Petco Animal Supplies Inc.
PetSmart Inc.
Philips Electronics N.V.
Pier 1 Imports Inc.
Planet Shoes
PrintingForLess.com Inc.
❷ PromGirl LLC
Purchasing Power LLC
PureFormulas.com
QVC Inc.
❸ Ralph Lauren Media
Real Real Inc.
RealTruck.com
Redbox Automated Retail
REI
Rent the Runway Inc.
RepairClinic.com Inc.
❸ Replacements Ltd.
Rock Bottom Golf
❸ RockAuto LLC
Sears Holdings Corp.
❸ Sephora USA Inc.
Shindigz
Shoebuy.com Inc.
ShopLadder
ShoppersChoice.com
❷ Signet Jewelers Ltd.
Skechers USA Inc.
Smarthome Inc.
❹ Sonic Electronix
Spanx Inc.
❷ **SparkFun Electronics**
Sports Authority
Spotify
❷ Spreadshirt Inc.
Stroll LLC
Stuart Weitzman LLC
❷ Sweetwater
❸ SwimOutlet.com
Tempur-Pedic
The Children's Place
The Clymb
The Finish Line Inc.
The Grommet
❹ The Gymboree Corp.
The Honest Company Inc.
❸ The Lakeside Collection
The Orvis Co. Inc.
❹ ThinkGeek Inc.
❸ Threadless.com
❹ Tiffany & Co.
Tilly's Inc.
Tire Rack Inc.
TJX Cos. Inc.
TOMS Shoes Inc.
❸ Tory Burch LLC
Touch of Modern Inc.
❷ Tumi Inc.
Turn5 Inc.
Ulta Beauty
UnbeatableSale.com Inc.
❷ Under Armour Inc.
Uniqlo USA Ltd.
VF Corp.
❷ Vintage Tub & Bath
VitaminShoppe.com
❹ Walmart.com
Warby Parker
❸ Wayfair LLC
❸ Weight Watchers
West Marine Products
Yoox Group
Zazzle Inc.
❸ zulily Inc.
Zumiez Inc.

Bold – 2015 OTA Top 10 Online Retailer

❷ ❸ ❹ – Number of consecutive years as an Online Trust Honor Roll recipient