2013 Online Trust Honor Roll & Online Trust Index - Appendix

Independent Audit of Best Practices In:

- Domain, Brand & Consumer Protection
- Site, Server & Infrastructure Security
- Data Protection, Privacy & Transparency

June 5, 2013

OTA
Online Trust Alliance

Table of Contents

APPENDIX A - 2013 OTA HONOR ROLL RECIPIENTS – INTERNET RETAILER 500

Internet Retailer 500 - Honor Roll		
1-800 Contacts Inc.	Etsy Inc.	Onlineshoes.com
AC Lens	evo	**OpticsPlanet Inc.**
Action Village Inc.	**Fathead LLC**	**Overstock.com Inc.**
Alibris Inc.	Fossil Inc.	Pacific Sunwear of California Inc.
Amazon.com Inc. *	Furniture.com Inc.	**Payless ShoeSource Inc.**
American Greetings Corp. *	Gaiam Inc.	**PersonalizationMall.com**
American Musical Supply Inc.	**GameStop Corp.**	Philips Electronics N.V.
Amway Global	**Garmin Ltd.**	**Powell's Books Inc.**
Ancestry.com Inc.	Geeks.com	RadioShack Corp.
Apple Inc.	Groupon Inc.	Rakuten.com Shopping (was Buy.com)
Art.com Inc.	**Gymboree Corp., The**	Ralph Lauren Media LLC *
Avon Products Inc.	**Hat World Inc.**	**Replacements Ltd.**
Bass Pro Outdoor Online LLC	**Hayneedle Inc.**	RockAuto LLC *
Beau-Coup Favors Inc.	HP Home & Home Office Store	Sally Beauty
Bellacor Inc.	**HSN Inc.**	School Specialty Online
Best Buy Co.	Hulu LLC	Sephora USA Inc.
Beyond the Rack	Ice.com Inc.	Sheplers Inc.
Biblio Inc.	**ideeli Inc.**	**Shoes.com Inc.,** a sub of Brown Shoe Co.
Bidz.com Inc.	**iHerb Inc.***	**ShopNBC.com**
Big Fish Games Inc. *	JackThreads.com *	**Sierra Trading Post Inc.**
BikeBandit.com *	Jeffers Inc.	**Skechers USA Inc.**
Blockbuster Inc.	**K&L Wine Merchants**	Smarthome Inc.
Boats.net	Karmaloop.com	**Sonic Electronix**
Books-A-Million Inc. *	**Kohl's Corp.**	SonyStyle.com (Sony Electronics)
Build.com Inc.	**Lakeshore Learning Materials**	Sports Authority Inc., The
BuildASign.com	Lakeside Collection	SportsMemorabilia.com LLC
Cabela's Inc.	**Lamps Plus Inc.**	SwimOutlet.com
CafePress.com	LeatherUp.com	**ThinkGeek Inc.**
Camping World Inc.	LEGO Brand Retail Inc.	Threadless.com
Columbia Sportswear Co.	Levenger Co. *	**Tiffany & Co.**
Crate and Barrel	Liberty Media Corp. (QVC, Liberty E-Comme	Tilly's
CustomInk.com	**LifeWay Christian Resources**	Tory Burch LLC
Cymax Stores Inc.	**Living Direct Inc.**	Totsy.com
DailyGrommet.com	LivingSocial Inc. *	**Touch of Class**
dELiA*s Inc.	Lowe's Cos. Inc.	**Vitacost.com Inc.**
Dell Inc.	**Microsoft Corp.**	**Walmart.com**
Dermstore LLC	Minted.com	Wayfair
Discount Dance Supply	**ModCloth Inc.**	Weight Watchers International Inc.
Discount Ramps.com LLC	**Net-a-Porter LLC**	Wine.com Inc.
Disney Shopping Inc.	**Netflix Inc. ***	Yankee Candle Co. Inc., The
e.l.f. Cosmetics	New Balance	**Zazzle Inc.**
Edible Arrangements International LLC	NoMoreRack.com Inc.	Zulily Inc.
Entertainment Earth Inc.	Northern Tool + Equipment Co.	

*Bold = 2012 & 2013 Honor Roll , * = 2013 Top 10 scoring Internet Retailers*

Data Source – The Internet Retailer 2013 Top 500 Guide®. Ranking based on revenues. Published May 2013. http://www.internetretailer.com/top500guidesuite/

APPENDIX B - 2013 OTA HONOR ROLL RECIPIENTS – FDIC 100

2013 FDIC Top 100 - Honor Roll	
American Express Bank, FSB.	Morgan Stanley Bank, NA
American Express Centurion Bank	Morgan Stanley Private Bank, NA
Bank of America California, NA	**Scottrade Bank**
Bank of America Oregon, NA	SunTrust Bank
Bank of America, NA	**The Frost National Bank**
Bank of America, Rhode Island, NA	**U.S. Bank NA**
BMO Harris Bank NA	UBS Bank USA
Charles Schwab Bank	**USAA Federal Savings Bank**
Citibank, NA	USAA Savings Bank
E*TRADE Bank	**Wells Fargo Bank Northwest, NA**
FIA Card Services, NA	**Wells Fargo Bank South Central, NA**
First National Bank of Omaha	**Wells Fargo Bank, NA**
HSBC Bank USA, NA	

Data Source: Federal Deposit Insurance Corporation (FDIC) December 2012 report on top 100 FDIC member banks based on assets (Note: FDIC tracks banks based on their State charter. In some cases banks use separate domains or subdomains, while in other cases they resolve to the parent corporation). **Bold** indicates 2012 and 2013 Honor Roll Recipient.

APPENDIX C - 2013 OTA HONOR ROLL RECIPIENTS – SOCIAL 50

2013 Social 50 - Honor Roll	
AOL	Instagram
Badoo.com	**LinkedIn**
Blogger	Naver.com Cafe
deviantArt	**Odnoklassniki**
eHarmony	**Orkut**
Facebook	Pinterest
FiveRR	PlentyofFish
Flickr	Tagged
Foursquare	**Tumblr**
Goodreads	**Twitter**
Google Plus	Wordpress
HI5	YouTube
ImageShack	**Zynga Inc.**

Source: Based on site traffic as reported by comScore http://www.comscore.com/ and Alexa http://www.alexa.com/topsites Social categories include social networking, image sharing, blogging, dating and gaming sites. **Bold** indicates 2012 and 2013 Honor Roll Recipient.

APPENDIX D - 2013 OTA HONOR ROLL RECIPIENTS – OTA MEMBERS

2013 OTA Members - Honor Roll	
Act-On Software	**Marketfish**
American Greetings Interactive	**Marketo**
Agari	**MarkMonitor**
Basegrow	Message Systems
bounce.io	**Microsoft**
comScore	**NSS Labs, Inc.**
Constant Contact	**Online Trust Alliance (OTA)**
deviantArt	**PayPal, Inc.**
DigiCert	**PrivacyChoice**
e-Dialog	**Publishers Clearing House (PCH)**
eHarmony	PwC (PricewaterhouseCoopers)
Ensighten	**Responsys**
Epsilon	**Return Path**
eWayDirect	RiskIQ
ExactTarget	**Sailthru**
GetResponse	**Silverpop**
GlobalSign	**SimplyCast**
Go Daddy	SiteLock
Harland Clarke Digital	**Symantec**
High-Tech Bridge SA	**TRUSTe**
ICONIX	**TrustSphere**
Identity Guard	**Twitter**
Innovyx	Verisign, Inc.
(IID) Internet Identity	VivaKi
Intersections Inc.	**ZEDO, Inc.**
Listrak	**Zynga Inc.**
MailChimp	

OTA Member Honor Roll – Member companies as of April 30, 2013.

Bold indicates 2012 and 2013 Honor Roll Recipient.

APPENDIX E - SECTOR DEFINITION AND SUMMARY ANALYSIS

INTERNET RETAILER (IR 500)

The data for ecommerce sites is from the Internet Retailer 2013 Top 500 Guide®, a ranking of the largest North American e-retailers by online sales, produced by Vertical Web Media, publisher of *Internet Retailer* magazine. Consistent with past reports, the top 100 (IR 100) have been segregated from the total 500 (IR 500), looking for trends of the largest companies while providing comparability to other segments.
http://www.internetretailer.com/top500guidesuite/

Internet Retailer 100				
	2010	**2011**	**2012**	**2013**
Email Authentication (Any)	76.0%	84.0%	97.0%	96.0%
Any SPF	63.0%	65.0%	67.0%	85.0%
Any DKIM	37.0%	55.0%	82.8%	87.0%
Email Authentication (Both)	24.0%	42.0%	55.6%	76.0%
SSL Average	-	-	75.88	85.33
EVSSL	18.0%	27.3%	27.2%	28.0%
Privacy Score (Average)	-	-	61.16	62.97
Privacy Score (Median)	-	-	60.00	65.50

Internet Retailer 500				
	2010	**2011**	**2012**	**2013**
Email Authentication (Any)	54.3%	64.9%	90.6%	88.0%
Any SPF	46.7%	50.5%	62.5%	78.6%
Any DKIM	22.8%	33.4%	69.5%	65.0%
Email Authentication (Both)	14.4%	23.0%	43.0%	55.6%
SSL Average	-	-	76.77	85.11
EVSSL	26.1%	29.8%	30.7%	33.4%
Privacy Score (Average)	-	-	63.48	64.36
Privacy Score (Median)	-	-	67.00	68.00

FDIC 100 - Based on a ranking of financial institutions by their total assets as reported by the FDIC as of December 31, 2012. Note several of the banks are individual State-chartered banks yet owned by the same parent, and in some cases resolving to the same web address.

FDIC 100				
	2010	**2011**	**2012**	**2013**
Email Authentication (Any)	55.0%	58.9%	69.0%	77.0%
Any SPF	49.0%	50.0%	60.0%	76.0%
Any DKIM	29.0%	34.4%	44.0%	50.0%
Email Authentication (Both)	22.0%	23.3%	34.0%	49.0%
SSL Average	-	-	75.84	85.04
EVSSL	25.6%	45.6%	55.0%	60.0%
Privacy Score (Average)	-	-	58.52	61.12
Privacy Score (Median)	-	-	50.00	50.00

SOCIAL 50 - Data was provided by comScore and Alexa based on site traffic as of April 15, 2013. Of the top 50, the top 5 sites account for more than 70% of the traffic worldwide. The 2013 list was expanded from 30 to 50 sites to include top image and document sharing, blogging, gaming and dating sites.

Social 50			
	2011	**2012**	**2013**
Email Authentication (Any)	92.0%	96.3%	98.0%
Any SPF	88.0%	96.3%	96.0%
Any DKIM	52.0%	63.0%	74.0%
Email Authentication (Both)	28.0%	63.0%	72.0%
SSL Average	-	77.72	82.14
EVSSL	12.0%	29.6%	24.5%
Privacy Score (Average)	-	78.81	76.20
Privacy Score (Median)	-	82.00	79.50

FEDERAL 50 - Site selection for this group was based on several criteria including ranking of site traffic as provided by comScore and past evidence of having been targeted by spoofing attempts, phishing exploits and email forgery. Additional criteria included those agencies commonly considered to be citizen-facing and identified as at-risk by the U.S Department of Homeland Security.

Federal 50				
	2010	**2011**	**2012**	**2013**
Email Authentication (Any)	32.0%	38.0%	58.0%	72.0%
Any SPF	30.0%	36.0%	50.0%	68.0%
Any DKIM	4.0%	6.0%	18.0%	24.0%
Email Authentication (Both)	2.0%	4.0%	10.0%	20.0%
SSL Average	-	-	67.73	73.15
EVSSL	11.4%	22.2%	25.9%	15.2%
DNSSEC	-	70.0%	70.0%	88.0%

OTA MEMBER COMPANIES

The list was based on members as of April 30, 2013. Member companies are posted at https://otalliance.org/about/Members.htm. Analysis focused on private sector businesses and sites excluding OTA Professional members, NGOs, non-profits and government agencies. Note: OTA member companies agree to make best efforts to adopt prescribed best practices within 12 months of joining. This pledge is reflected in OTA member scores which are generally higher than those found in individual industry sectors.

OTA Members				
	2010	**2011**	**2012**	**2013**
Email Authentication (Any)	88.0%	95.3%	98.6%	100.0%
Any SPF	83.3%	95.3%	98.6%	100.0%
Any DKIM	22.0%	34.5%	57.1%	68.8%
Email Authentication (Both)	36.0%	43.8%	58.6%	68.8%
SSL Average	-	-	79.77	87.10
EV SSL	32.5%	35.3%	43.4%	35.0%
Privacy Score (Average)	-	-	78.90	83.70
Privacy Score (Median)	-	-	81.00	85.00

APPENDIX F – METHODOLOGY

The 2013 Honor Roll includes a composite analysis of a site's security and privacy practices focusing on three major categories, including fourteen separate criteria. Sites were eligible to receive 300 total points across the three categories as well as up to 25 bonus points for adoption of leading-edge practices.

The categories include:

1) Domain, Brand & Consumer Protection
2) Site, Server & Infrastructure Security
3) Data Protection, Privacy & Transparency

The 2013 report expands the criteria and provides additional weight and granularity to key practices. Sites which received a composite score of 80% or better and a score of at least 55 in each of the three categories qualified for the 2013 Honor Roll. Data sampling of survey sites, their DNS, email and privacy policies were completed between April 21 and May 20, 2013. In total, more than 500 million emails were examined and approximately 10,000 web pages reviewed.

To drive adoption of best practices, OTA published the 2013 criteria in early January, 2013 on the OTA website and included mention in our public newsletters, third party webinars and social media including Twitter, LinkedIn and Facebook. As a result of OTA's public posture and announcement of testing plans at events and webinars, several sites contacted OTA indicating they were in the midst of upgrading their infrastructure and adopting prescribed best practices. To assure a level playing field, all subject domains were re-evaluated the week of May 13 to check for infrastructure updates, changes to online data collection, and improvements to email authentication.

It should be noted that this research is based on a "slice of time" and individual companies may have since adopted or changed their security and privacy practices. We also recognize that the sites examined might be using other technologies (which our tools or research did not detect) to authenticate domains or subdomains, secure their infrastructures, track users on their sites, etc.

Due to the sensitivity of this data and risk of disclosing vulnerabilities, individual organization's scores and data are not publically available. Information will be provided to site owners upon written request and verification. For details, including reporting fees, please send an email to staff@otalliance.org.

APPENDIX G – COMPONENTS OF THE COMPOSITE SCORES

DOMAIN, BRAND & CONSUMER PROTECTION

Email Authentication (SPF & DKIM) – The report analyzed more than 500 million emails and the DNS infrastructure of leading sites and subdomains. It assessed efforts to protect users from domain and email spoofing via the adoption of SPF and DKIM. Sites received maximum scores by implementing both SPF and DKIM, as well as, implementing authentication at the top level domain (i.e. yourdomain.com) and publishing DMARC records with a reject or quarantine policy, (see below). Verification of DKIM-signed email required review of the email headers of individual emails via sampling providing by Agari, Microsoft, Return Path and TrustSphere. Results were integrated into the composite scoring and factored as a component of the baseline points required to qualify for the Honor Roll. Verification of SPF records was completed using the OTA web tool posted at, https://otalliance.org/resources/authentication/spflookup.html.

Domain-based Message Authentication, Reporting & Conformance (DMARC) – DMARC standardizes how email receivers perform email authentication using the SPF and DKIM mechanisms. Sites that have published DMARC records receive a positive score with additional scoring for sites that have published a "reject" or "quarantine" policy. DMARC details are posted at https://otalliance.org/resources/authentication/dmarc.html. Verification was completed using the OTA DNS query tool, https://otalliance.org/resources/authentication/spflookup.html.

Domain Locking - Domain locking is a free security enhancement offered by most registrars to help prevent unauthorized transfers of your domain to another registrar or web host by locking your domain name servers. When your domain is locked, you'll be substantially protected from unauthorized third parties who might try to redirect your name servers or transfer your domain without your permission. Sites receive negative points if their domain is not locked. For more information visit, http://support.godaddy.com/help/article/410/locking-and-unlocking-your-domain-names

SITE, SERVER & INFRASTRUCTURE SECURITY

SSL Server Configuration – Sites were evaluated using a combination of data from Qualys SSL Labs (https://www.ssllabs.com/ssltest) and analysis by High-Tech Bridge SA. These tools provide visibility into the server architecture, configuration and digital certificate. Test evaluated for weak keys, protocols, algorithms, and server misconfigurations that can enable attackers to exploit system vulnerabilities and compromise SSL communications. Note the SSL Labs tool was substantially updated in February 2013. Details are posted at, https://community.qualys.com/blogs/securitylabs/2013/02/07/ssl-labs-update-increases-security-requirements.

Extended Validation SSL Certificates (EV SSL) – As explained in Appendix I, EV SSL offers trust mechanisms visibly confirming the identity of the site to the user. The 2013 analysis focused on all sites with SSL connections, no longer limiting the evaluation to only consumer facing e-commerce or banking sites. This change is the result of the increased focus of cybercriminals targeting business-to-business, social networking and government sector sites. Sites that have implemented EV SSL Certificates receive bonus points. https://otalliance.org/resources/EV/index.html.

Always On SSL (AOSSL) – AOSSL is a best practice to secure sensitive data, especially for users of public Wi-Fi hot spots. With the advent of widely available tools, criminals can "sidejack" cookies and data packets from unsuspecting users. Sidejacking allows hackers to intercept cookies (typically used to retain user-specific information such as username, password and session data) when they are transmitted without the protection of SSL encryption. Sites supporting AOSSL receive additional points. This capability was measured using the Qualys SSL Server Test to look for Strict Transport Security and verified by auditors accessing the sites. https://otalliance.org/resources/AOSSL.

2048 bit key or Elliptic Curve Cryptography (ECC) Certificates – Sites that have adopted 2048-bit certificates or ECC receive bonus points. ECC adds security to SSL Certificates, offering a secure web experience that is favorable to users and can reduce server and virtual server overhead needs for processing connections. ECC supports the National Institute of Standards and Technology (NIST) requirement to migrate from RSA 1024-bit crypto to 2048-bit certificates by January 2014. More info at https://otalliance.org/resources/SSL/ECC.html.

Domain Name System Security Extension (DNSSEC) – Testing for DNSSEC was completed using a tool from Verisign Labs http://dnssec-debugger.verisignlabs.com/ which queries the DNSSEC records. Sites adopting DNSSEC receive bonus points. https://otalliance.org/resources/dnssec.html.

DATA PROTECTION, PRIVACY & TRANSPARENCY

Privacy Policy – Using third-party data from Privacyscore (www.privacyscore.com), a service of AVG Technologies, and additional OTA criteria, sites were analyzed for their privacy policy and data collection practices. A Privacyscore evaluates privacy risk based on a website's published policies about protection of personal data and the privacy qualifications of third-parties seen to be collecting data on the site. Website privacy policies regarding sharing, deletion, disclosure notices and vendor confidentiality were reviewed by analysts during the period between April 21 and May 20, 2012. Privacyscores for third-party tracking companies (reflecting policies on anonymity, boundaries, choice, retention and oversight) were weighted based on their prevalence in site scans. Sites were crawled for a period of over 96 hours to observe data collection and onsite tracking. It is importance to note and recognize Privacyscores can frequently change over time based on the mix of third-party tracking and revisions to privacy policies. Results from Privacyscore were integrated into the composite scoring and factored as a component of the baseline points required to qualify for the Honor Roll. For a complete review of the Privacyscore methodology, review the FAQ at, http://www.privacyscore.com/faq.

Third Party Tracking on Site (incorporated into Privacyscore – see above)

Honoring of Do Not Track Browser Settings (DNT) – Websites which publically disclose the status of honoring or not honoring the browser-based DNT setting receive bonus points. Such an assertion would be in addition to any such notice a user is presented when visiting a site and does not preempt any such notice. A DNT signal asserts a user's request to not collect and share their online data. Composite scores for sites with no assertion to support or ignore the DNT signal will not be impacted. As the standard is evolving with the W3C, it is recognized that many sites are reviewing their position. Currently, proposed support of DNT by a site is voluntary.

Public vs. Private WHOIS registration – Sites that are registered by proxy or private registration received a negative score, reflecting a lack of transparency. While it is recognized that sites may choose to opt-in for private domain name registration, public facing sites are discouraged from doing so and consumers should exercise caution when interacting with sites that have made their domain information private. Results were integrated into the composite scoring as a negative score for sites with private registrations and factored as a component of the baseline points required to qualify for the Honor Roll, http://who.godaddy.com/?prog_id=GoDaddy

Data Breach & Loss Incidents – Companies who have experienced a data breach or a data loss incident since April, 2011 received negative points. See 2013 OTA Data Protection & Breach Readiness Guide, https://otalliance.org/news/releases/2013DataBreachGuide.html.

FTC / State Settlements – Companies which have been in violation of the FTC Act including settlements and judgments since April, 2011 receive negative points. The FTC Act focuses on consumer protection, including but not limited to deceptive advertising, privacy and data security practices. See http://business.ftc.gov/legal-resources/8/.

APPENDIX H – OVERVIEW OF EMAIL AUTHENTICATION & DMARC

In early 2004, several promising industry initiatives emerged to help address the threats of deceptive email, phishing and spam. Working through the standards community and with broad industry and business input these initiatives produced two key email authentication technologies that allowed senders to be verified: Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM). Mailers, receiving networks and ISPs worldwide have found that adoption of both SPF and DKIM yields the highest value versus utilizing either independently.

The role of email authentication can best be seen in step 3 above, where the identity of incoming messages is verified by checking the SPF DNS records and DKIM keys. When an assessment of the sender's reputation (step 4) is added, receiving networks reduce false positives and maximize the deliverability of legitimate email. In general, because spammers can easily authenticate their email, OTA cautions against applying inbound email authentication results without reputation data (domain or IP) as the sole method of distinguishing legitimate email.

To raise awareness of the value of email authentication, in April 2005 OTA published an initial report highlighting email authentication best practices.[1] Each successive report has included additional detail about adoption of these key authentication technologies across a variety of industry sectors.

[1] https://otalliance.org/news/releases/F500_reportcard.html

APPENDIX I - EXTENDED VALIDATION SSL CERTIFICATES

Extended Validation SSL Certificates (EV SSL) were introduced in 2006 to help combat phishing sites and look-a-like sites that attempt to spoof high-value targets like banks, social networks, and online retailers. Extended validation makes it harder for a criminal to fraudulently obtain an SSL Certificate. EV SSL requires a thorough identity verification process that helps prevent deceptive and illicit entities from obtaining a certificate.[2]

EV SSL Certificates provide differentiation and recognition to the organizations that obtain and publish them via SSL authentication on the web. This differentiation is highlighted by displaying a green identifier or other visual trust indicator in the browser chrome (not just the web page). EV SSL is supported by all leading browsers including Internet Explorer, Firefox, Chrome, Opera and Safari as illustrated below.[3] The incremental cost of an EV certificate is relatively small and is increasingly becoming an important part of a site's overall strategy of offering end users a visual trust indicator and enhanced web site security.

[2] Through a verification and audit process, Certificate Authorities require several documents including: 1) proof of registration within the applicant's jurisdiction, 2) independent third-party verification of the applicant's physical address, phone number and of all supporting documents, 3) verification of applicant's ownership of domain name(s) via data in the "Who Is" database, and 4) verification that the applicant and signer are authorized agents of the applicant. These documentation procedures can be easily accomplished by virtually any organization. For more information visit the CAB/Browser Forum at https://www.cabforum.org/index.html.

[3] Note Browser user interfaces may have changed since the release of this report. Check with your browser for updates.

APPENDIX J – HISTORY OF THE OTA HONOR ROLL

The genesis of the OTA Honor Roll started in 2005, as a scorecard focused on the Fortune 500 and email authentication to counter spoofed and malicious email. Today it has evolved to an independent audit including a composite analysis of over 750 websites and a dozen data elements evaluating a site's brand protection, site security and privacy practices.

2005 – First score card published https://otalliance.org/news/pressrelease.html

2006 - https://otalliance.org/news/summit_recap_050306.html

2007 - https://otalliance.org/news/F500leaders3_6.html

2008 - Scope expanded to include DKIM, (DomainKeys Identified Mail). Target segments were expanded to the Fortune 500, Internet Retailer 300, top 100 FDIC member banks and top ranked U.S. Federal Government banks and financial institutions. https://otalliance.org/news/releases/AOTA-authentication.html

2009 - Report expanded to include SSL and site security. https://otalliance.org/news/releases/F500_reportcard.html

2010 - Honor Roll concept introduced, focused on providing recognition to early adopters. Email authentication expanded to look at SPF record types and use of DKIM at both TLD and subdomains. https://otalliance.org/news/releases/2010honor_roll.html

2011 - OTA members and top ranked social sites were added. DNSSEC added for U.S. government sites. Increased focus on the importance of sites adopting both SPF and DKIM. https://otalliance.org/news/releases/2011scorecard.html

2012 - Introduction of the Online Trust Index (OTI), as a comparative metric across key market segments and industries. The report was expanded to analyze sites' SSL implementation using tools from Qualys SSL Labs, as well as privacy practices and policies utilizing data provided in part by PrivacyChoice. Added Always On SSL (AOSSL) and DMARC as bonus scores, with weighting applied to sites who published "reject" or "quarantine" policies. Evidence of data breaches, WHOIS private registrations and past FTC settlements or fines were included in the composite analysis. https://otalliance.org/news/releases/2012HonorRollRelease.html

2013 - The Honor Roll audit process has become more rigorous, requiring a combined score of 80% or above and a minimum score of 55 in each major category. Weighting of email authentication has shifted to focus on the importance of adoption at the corporate domain level, addressing brand protection and the risk of spearphishing. DMARC moved from a bonus score to a baseline component of the scoring. SSL analysis evolved to address current attack vectors, with bonus points added for sites who have adopted 2048-bit certificates. SSL analysis was also enhanced with additional data and vulnerability assessments from HighTech Bridge SA.

APPENDIX K – RESOURCES

2013 Honor Roll Report Updates & Appendix
https://otalliance.org/2013HonorRoll.html

Anti-Botnet Initiative
https://otalliance.org/resources/botnets/index.html

Anti-Malvertising
http://otalliance.org/resources/malvertising.html

Always On SSL
https://otalliance.org/resources/AOSSL/index.html

DNSSEC
http://otalliance.org/resources/dnssec.html

Email & Domain Authentication
http://otalliance.org/resources/authentication/index.html

Extended Validation SSL Certificates
https://otalliance.org/resources/EV/index.html

Online Trust Principles
http://otalliance.org/resources/principles.html

Data Breach Readiness Plan
http://otalliance.org/resources/Incident.html

Standardized Data Collection & Privacy Statement
http://otalliance.org/privacy_demo.html

Top Tips To Help Protect Your Site & Customers
https://otalliance.org/news/releases/2012Top10.html

OTA Glossary
https://otalliance.org/resources/OTA%20Glossary.pdf

Revised June 5, 2013
v1