APPENDIX E – BEST PRACTICE CHECKLIST

DNS, Domain, Brand & Consumer Protection		
❑	SPF records & DKIM at the corporate and sub domains	Base Score
❑	DMARC records with reject/quarantine policy	Base Score
❑	Naked DMARC records (p=none and no RUA or RUF)	Invalid
❑	Opportunistic TLS for email	Bonus Points
❑	Implement DNSSEC	Bonus Points
❑	IPv6 Adoption	Bonus Points
❑	Multi-Factor Authentication	Bonus Points
❑	Domain locked	Penalty for not locking
❑	Inbound email authentication and DMARC checking	Not scored; recommended
Site, Server & Infrastructure Security		
❑	Server Security & Configuration	Base Score – aggregate, multiple tests
❑	SSL/TLS Certificate, Protocol, Key Exchange, Ciphers	Base Score – aggregate, multiple tests
❑	Server Patching Cadence	Base Score
❑	Certification Authority Authorization (CAA)	Not scored, recommended (planned for 2018)
❑	Certificate Type (EV SSL)	Bonus Points
❑	Always on SSL (https by default)	Bonus Points
❑	Web Application Firewall	Bonus Points
❑	Malware, malicious links, malvertising incident	Penalty
❑	Anti-Bot Protection	Penalty for failure to have protection
❑	XSS / iFrame Vulnerability	Penalty
❑	Vulnerability / Bug Reporting Mechanism	Bonus Points
❑	DDoS Mitigation Mechanisms	Not scored, recommended (planned for 2018)
Privacy Policy, Tracking, Transparency & Disclosures		
❑	Link to privacy policy on home page	Base Score
❑	Privacy policy date stamp at top of page	Base Score
❑	Layered short notice design (links/expand sections)	Base Score
❑	Children's Online Privacy Protection Act (COPPA)	Base Score
❑	"Do Not Track" (DNT) disclosure	Base Score
❑	Data retention statement	Base Score
❑	Personal data not shared without permission	Base Score
❑	Vendors contractually held to privacy policy	Base Score
❑	Archived/prior version of privacy policy available	Bonus Points
❑	Icons used to clearly identify sections	Bonus Points
❑	Multi-lingual policy option clearly linked	Bonus Points
❑	Honor DNT browser setting	Bonus Points
❑	Disclosure of cross-device tracking	Bonus Points
❑	Tag Management System (TMS) in place	Bonus Points
❑	Notify if personal data is requested by 3rd party	Bonus Points
❑	Presence of 3rd Party tracking tags	Penalty, number of trackers
❑	Data breach reported	Penalty, number of incidents
❑	FTC/FCC/CFPB/State enforcement action	Penalty, number of settlements
❑	Is your WHOIS record Private?	Penalty