Executive Summary

Who can and cannot be trusted online is a problem as old as the Internet itself. The challenges of ensuring the integrity of online communications and transactions are amplified by the mass adoption of e-commerce, online banking, and Web 2.0 communications and services (see Exhibit 1 on next page). Economies with high levels of online activity—such as the United States where two-thirds of consumers now shop online—present a target-rich environment for cybercriminals and purveyors of online fraud. These factors put online consumers on edge: 44 percent of consumers say they’re less likely than they were a year ago to trust a Web merchant with personal data. And more than half of consumers (55 percent) have experienced security incidents that caused them to think twice about using an e-commerce Web site.

To allay consumer fears and boost confidence, many online businesses use trust marks—seals, logos and icons displayed on a Web site that provide information about what steps an online merchant is taking to protect its customers. These logos, often displayed prominently on a company’s home page, or during the checkout phase of a transaction, can indicate a range of things, including:

• Whether or not the company uses certain levels of encryption technology to help protect the information being transmitted over the Internet

• If the company is a legitimate, accredited business

• How thoroughly, if at all, the company’s Web site is scanned for vulnerabilities that could be exploited to steal data and identity information from customers

In general, trust marks are a form of communication between consumers and businesses to help bridge the information gap about the security and trustworthiness of an online store. They are especially important for e-commerce where merchants and buyers rarely meet or know each other beyond their digital identities. However, trust marks are only as good as the technology and policy behind them. Additionally, they are only as useful as a consumer’s awareness of a trust mark program’s strengths and weaknesses. This Yankee Group report defines the various types of trust marks, what they can and cannot do, and how consumers and businesses should use them.
Table of Contents

I. The State Of E-Commerce Security 3
   Trends in Consumer and SMB Online Activity 3
   Security Concerns of SMBs and Their Consumers 3
   Ever-Present Threats: Phishing, Web Malware and the Identity Theft Industry 4

II. Trust Marks: What They Are and How They Work 4
   Types of Trust Marks 5

II. Conclusions and Recommendations 8
   Recommendations 9

---

Exhibit I.
E-Commerce Nation: Two-Thirds of U.S. Consumers Shop Online
Source: Yankee Group, 2009

<table>
<thead>
<tr>
<th>Activity</th>
<th>Percent of Respondents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Search (e.g., Google)</td>
<td>76</td>
</tr>
<tr>
<td>Maps</td>
<td>69</td>
</tr>
<tr>
<td>Shopping</td>
<td>64</td>
</tr>
<tr>
<td>Auctions (e.g., eBay)</td>
<td>46</td>
</tr>
<tr>
<td>Local Event Listings</td>
<td>45</td>
</tr>
<tr>
<td>Instant Messaging</td>
<td>42</td>
</tr>
<tr>
<td>Classifieds (e.g., Craigslist)</td>
<td>33</td>
</tr>
<tr>
<td>Social Networks (e.g., MySpace)</td>
<td>33</td>
</tr>
<tr>
<td>Web Video (e.g., YouTube)</td>
<td>31</td>
</tr>
<tr>
<td>Video Games</td>
<td>31</td>
</tr>
<tr>
<td>Blogs</td>
<td>28</td>
</tr>
<tr>
<td>Photo Sharing (e.g., Flickr)</td>
<td>25</td>
</tr>
</tbody>
</table>

n= 1,500 U.S. consumers
I. The State Of E-Commerce Security

Trends in Consumer and SMB Online Activity

Online financial transactions are now commonplace for most consumers, according to the Yankee Group Anywhere Consumer: 2008 U.S. Web/Data Survey. More than 60 percent of U.S. consumers said they bought goods online in the past month, and 70 percent said they use their bank’s electronic banking feature. A significant minority (30 percent) also participate in other online financial transactions, such as auctions.

Consumers are not naive about the security issues involved with online transactions and e-commerce; they are more aware now than ever of the importance of online security and safety. Yankee Group research shows that 86 percent of all consumers use some kind of anti-virus software on their PCs. Also, 80 percent of consumers said that it is important for them to keep this software up-to-date with an annual subscription service. Anti-spam and anti-spyware usage is also strong among consumers, with adoption rates of around 80 percent and 60 percent, respectively.

Although consumers are more likely drawn to the Web sites of giant “e-tailers”—the Amazons, Apples, eBays and Dells of the Web world—small and medium businesses (SMBs), which are firms Yankee Group defines as having less than 500 employees, are increasingly looking to the Web to sell products and connect with customers. According to the Yankee Group Anywhere Enterprise—Small and Medium: 2008 U.S. Mobility and Business Applications Survey, one-third of SMBs in the U.S. currently sell products online or use e-commerce as a business tool. Another 26 percent say they have plans to follow suit in the next 12 months. With a majority of SMBs set to become e-commerce companies by next year, small businesses will be challenged to keep their customers’ identities and sensitive data secure.

Security Concerns of SMBs and Their Consumers

For SMBs, protecting critical data, such as customer lists and consumers’ personal information, is a dire challenge. A recent Consumer Reports survey showed 88 percent of online shoppers said that the protection of their personal data was their top concern; 71 percent of consumers indicated they think it is important that the Web site they do business with display some kind of trust seal or logo. That means that an SMB’s ability to show what steps it is taking to protect its customers’ identities can directly affect whether or not consumers will do business with it in the first place.

Online security breaches and data loss events have the potential to be devastating to an enterprise, particularly smaller businesses. Discount retailer TJ Maxx and e-brokerage TD Ameritrade lost more than 100 million customer credit card numbers combined in the last two years due to hacking attacks. But despite terrible media headlines, these two firms are still in business. Smaller companies have more to lose if their customers lose faith in the businesses’ Web site security. SMBs typically don’t have the brand equity or scale to weather a major data breach catastrophe. Unfortunately, among SMBs, data loss and exposure of customer data are the most common type of security breach. In fact, more than 15 percent of SMBs reported an accidental disclosure of customer data in 2008 (e.g., e-mailing a file to the wrong address, losing a laptop). Another 11 percent revealed they also had customer data stolen by an outside attacker as a result of a Web site hack or network intrusion. Such data loss events cause severe monetary damages to SMBs according to the Yankee Group 2007 Anywhere Access survey. Among SMBs that reported a data loss incident in 2007, 30 percent estimated the financial loss due to the breach was more than $500,000—a significant sum to a small to mid-size firm.

As for consumers, while their online shopping activity is high, they maintain an underlying distrust about the safety and security of Web shopping and the Internet. More than half of consumers (55 percent) said that recent security incidents they experienced caused them to consider possible security issues when visiting a Web site. This skepticism about Internet security makes consumers think twice about what personal information they are willing to give out over the Internet resulting in shopping cart abandonment, or whether they will do online business at all. To that end, 44 percent of consumers said they are less likely to trust a Web site with their personal data this year than they were last year.

55 Percent of U.S. consumers experienced online incidents that caused them to consider possible security issues when visiting a Web site.
Ever-Present Threats: Phishing, Web Malware and the Identity Theft Industry

It’s with good reason that consumers are more wary of the Internet as a safe medium for purchasing goods and services. Consumers face real monetary damages if their computers become infected with malware intended to steal personal data, or if their favorite online retailer’s site is hacked. The total dollar amount reported lost as a result of cybercrime is at an all-time high: $239 million as of 2007, which is a 30 percent jump from the amount of dollar-loss reported two years earlier, according to the FBI’s Internet Crime Complaint Center (IC3).

This points to a more focused and effective cybercriminal methodology for extracting money from victims. Reports are increasing of incidents in which even benign Web sites are injected with malware that can unknowingly be downloaded to end-user machines to scan for personal information, intercept keystrokes of passwords and then send this data back to a criminal outfit’s server. Throughout the last 18 months, news reports highlighted several such high-profile incidents, including:

- **The Super Bowl:** Hackers successfully inserted attack code onto the official Web site of the Miami Dolphins’ stadium, dolphinsstadium.com, during the week the facility was to host Super Bowl XLI. Vulnerable Microsoft Windows PCs accessing the site were exposed to malware which sent the visitors to a server in China, which infected their machines with data/identity-stealing malware.

- **Paris Hilton:** The celebrity’s personal Web site was compromised with malware that presented visitors with a pop-up window that forced them to download “viewing enhancement” software, which was actually malware.

- **Major League Baseball:** The official league Web site, MLB.com, was recently compromised for a second time when online advertisements the Web site was displaying from a third-party turned out to contain malware that was infecting MLB.com visitors who clicked on the ads.

So given this dangerous and threatening online environment, the basic question consumers and SMBs must ask is, “Who can you trust online?” One way online merchants help answer this question for consumers is by using a trust mark from a trusted third party. Trust marks and seals can be considered as a “Good Housekeeping Seal of Approval” for the e-commerce era. The key to such marks or logos is that they are offered by a trusted third party, which reviews the reputation, security or business practices of a company, and then authorizes that business to use the third party’s seal or mark. Such logos and seals on a Web site tell customers about a business’s Web security measures and overall business practices, and can reassure site visitors that the business is a trustworthy e-commerce entity.

II. Trust Marks: What They Are and How They Work

Trust marks most commonly take the form of a small insignia or button, often displayed on a Web site’s home page or checkout page. These marks make a variety of implicit or explicit claims, which may include:

- The mark claims to prove the overall **reputation** of a business behind the Web site. Such a seal shows the company meets criteria for basic and proper business practices, proof of the company’s incorporation, disclosure about its location, and that the firm has truth-in-advertising policies, and offers recourse for customer complaints.

- The mark claims to assure **privacy** about customers’ personal data. This may include the disclosure of a business’s policies about sharing customer data with external parties.

- The mark claims to promise to end users that their traffic is secured with encryption technology, such as **Secure Sockets Layer (SSL)**, a universal standard for encrypting online transactions.

- The mark claims to actively perform **security/vulnerability scanning**, which demonstrates that a Web site has been checked for Web-based intrusions, injections of malicious code or other vulnerabilities that hackers exploit to compromise a Web transaction and thus a customer’s personally identifiable information.

### Types of Trust Marks

| Reputation | A reputation trust mark claims to offer a baseline level of proof that there is an actual, legitimate business behind a Web site that follows proper business practices. |
| Privacy | A privacy trust mark shows that the merchant abides by a set of customer data management practices, as defined by the provider of the trust mark service. |
| Secure Sockets Layer (SSL) | A valid SSL trust mark ensures end users that the site uses SSL session encryption technology. |
| Security/Vulnerability Scanning | Denotes use of a regularly scheduled security auditing and vulnerability detection service for its Web site, aimed at ensuring the site is free of malware, viruses, malicious downloads and other types of spyware. |
Types of Trust Marks

These four types of trust marks—reputation, privacy, SSL and security/vulnerability scanning—fall into the categories of “soft” and “hard.” “Soft” marks claim that the business displaying the mark abides by the mark-provider’s code of conduct, typically requirements around privacy and business conduct. “Hard” security seals—including SSL and security/vulnerability scanning—denote the use of certain security technologies or auditing procedures. In this section, we examine what each of the four soft and hard trust marks do, analyze their general strengths and weaknesses, and describe what they should mean to consumers and businesses.

Reputation

What it is/what it does: A reputation trust mark claims to offer a baseline level of proof that there is an actual, legitimate business behind a Web site that follows proper business practices. Such an insignia can assure customers that the organization they are dealing with has a fixed address and telephone number, or that it has been in business for a certain amount of time. Among the most recognized in this area is the cyber arm of the Better Business Bureau, a 90-year-old nonprofit organization aimed at promoting sound, reputable business practices. The BBBOnline trust mark is for businesses that wish to show their practices and standards of conduct are in line with the BBBOnline’s requirements. Involvement in this program includes an initial—and periodically updated—vetting process to confirm that the company has a fixed mailing address in the United States or Canada, that the organization has been in business for at least one year, and it abides by overall BBB policies regarding customer complaint handling, truth in advertising practices and other stipulations.

Strengths and weaknesses: The reputation trust mark is as strong as the organization behind it. In the case of BBBOnline, the strength of the trust mark is the practices (discussed above) it requires of merchants before they can display the mark. However, online reputation trust marks are sometimes audited infrequently, meaning a Web site displaying the seal could have fallen out of compliance with the seal-provider’s requirements. Another weakness of this kind of mark is in its general “soft” nature, which is the lack of security technology behind the seal. Such seals do not indicate what, if any, encryption or vulnerability scanning measures a merchant may use to secure customer connections.

What it means for consumers: For consumers, the reputation trust mark is a starting point. Those interested in doing online business with a given company can look at a reputation trust mark as one signal that the company they’re dealing with is a legitimate enterprise. Consumers can also contact the reputation service directly via e-mail or phone to confirm that the Web site displaying a certain trust mark is an actual member of that organization’s service. This trust mark type does not show that the business has taken any technical steps to secure its site or any online transactions. To draw an analogy with the brick-and-mortar world, a reputation seal or logo in the shop window says nothing about how strong the locks are on the front door.

What it means for SMBs: A reputation trust seal can give an SMB a certain level of legitimacy and a more big-business image. The mark enables the small business to communicate to current and potential customers that it is reputable, and abides by good business practices and standards. It is not a guarantee or assurance of any technical aspect of the SMB’s Web site, such as whether or not the site is scanned regularly for vulnerabilities, or even if the site uses basic encryption technology for its sensitive transactions. The reputation seal on a Web site is the online equivalent of a shop or store displaying their local “Chamber of Commerce” sticker in the window or door.

Privacy

What it is/what it does: A privacy trust mark shows that the merchant abides by a set of customer data management practices, as defined by the provider of the trust mark service. Requirements typically include that a merchant post a privacy policy document on its site, outlining to customers what kinds of personal data the site may collect, and how this data might be used. The privacy seal provider may also require seal holders to provide Web site visitors with an “opt out” option for having their information shared with third-party organizations when customers are asked to provide personal data by a Web merchant. Disclosure of the use of cookies to track the Web site usage and history of a customer, and the subsequent sharing of that data, can also be required of an Web merchant wishing to display the privacy trust mark.
TRUSTe is an example of a widely used privacy trust mark program. Merchants that display this seal must abide by TRUSTe's data privacy best-practice requirements, which include the posting of a privacy policy document on the site, among other requirements. Displayers of the TRUSTe logo must also agree to participate in TRUSTe's complaint resolution service, which lets customers file disputes and complaints about the business displaying the logo. The BBBOnline program also provides privacy code assurances with a similar trust seal offering.

**Strengths and weaknesses:** The privacy trust mark suggests that a displaying merchant is aware of identity theft and personal data abuse issues. The posting of a privacy policy gives consumers information they can use to decide if they will conduct online business with a merchant. In the case of TRUSTe, such a logo also shows that site users will have recourse if they feel their privacy or personal data are abused.

However, the mark is not an iron-clad guarantee that merchant can, or will, keep customers’ data 100 percent private. It simply indicates that the displaying merchant claims it abides by the requirements of the trust mark provider. This is an important distinction, since these requirements can be somewhat open-ended and susceptible to loose interpretation by the merchant. For example, a seal provider may require a site to craft and post a privacy statement, but the provider may not necessarily be involved in the review of the policy itself. For example, a privacy statement that discloses that end users’ data may be sold or distributed without their consent could still be verified with a privacy trust mark in certain cases.

Additionally, the privacy seal does not guarantee that the site offers other types of security for visitors. For example, the privacy trust mark does not indicate any technical standard or process is used by the displayer, such as basic traffic encryption. (Although TRUSTe does require its seal holders to implement SSL for customer transactions, compliance tracking of this practice is not rigorous.) The privacy logo also makes no claims about Web infrastructure vulnerability testing and can still be vulnerable to hacking attacks.

*What it means for consumers:* Privacy seals are important to customers who fear their personal data might be shared with external parties without their consent. Consumers should know what is behind the privacy trust mark—the promise to abide by the privacy and best-practice requirements of the trust mark issuer. It is mostly a description of how the merchant will deal with a consumer’s online identity. The mark does not necessarily imply that specific technology is used to protect online shoppers from having their online identities stolen by determined thieves. In particular, consumers should consider not just the privacy policies the trust mark promises, but whether the trust mark provider has a system for compliance tracking in place, and whether the mark provider has a track record of compliance enforcement.

*What it means for SMBs:* For a small or midsize business, displaying a privacy logo on a Web site can assure consumers that a business is aware of consumers’ fears of identity theft and their concerns about how their personal data is used online. It can be a valuable measure of assurance for customers, especially for SMBs that plan to collect information about customers with marketing tools such as e-mail newsletters, frequent-buyers clubs, premium memberships, etc.

**Secure Socket Layer**

*What it is/what it does:* SSL is a session encryption technology that scrambles Web communications between a Web site and a browser/PC user, preventing hackers from intercepting confidential data, such as credit card numbers, or impersonating legitimate Web sites during transmission. Organizations that offer SSL certificates provide Internet merchants with an important technology for ensuring that a Web browser that supports SSL can talk to a company’s SSL-enabled Web server over an encrypted session. A valid SSL trust mark ensures end users that the site uses SSL session encryption technology. SSL also functions as a trust mark, typically displayed as an animated flash Web object. Some of these logos link back to the seal provider’s Web site, with information to verify that the logo is authentic and up-to-date, and that that Web merchant displaying the trust mark is using secure transmissions to handle confidential customer traffic.
The SSL logo is often displayed on home pages, as well as checkout submission pages, shopping cart sections of Web sites and other critical points in an online transaction where personally identifiable or financial information may be exchanged. VeriSign is the largest provider of SSL trust marks. Other providers include Trustwave, as well as dozens of other smaller providers.

**Strengths and weaknesses:** A valid SSL trust mark indicates that a site is using an up-to-date traffic encryption method for protecting information transmitted over the Web. However, the mark does not denote anything about the business or organization itself—its practices, reputation or customer data use policies—or how susceptible its site is to Web exploits and vulnerabilities. In other words, the SSL trust mark is an important, but minimal level of security assurance. Similar to a toaster marked with an Underwriters Laboratories (UL) insignia, the SSL can imply a basic level of safety.

Since SSL was first introduced in 1995, the technology has lost some luster as a gold standard for Web security measures. One factor contributing to this is the fact that not all certificate authorities are created equal, unfortunately; some have more lax standards for issuing SSL certificates, and the integrity of those certificates, than others. Also contributing to the erosion of SSL trust is the overall lax attitude consumers have toward SSL, particularly, SSL certificates that have expired or may not be as secure as necessary. Even Internet security pioneer and evangelist Bruce Schneier, in his January 2009 Cryptogram newsletter, admitted he often just clicks through an expired certificate warning on Web sites. Although the SSL trust mark conveys a level of technical security of a business’s Web site, it does not guarantee other areas of cybersecurity. For instance, even a Web site with an up-to-date certificate from a reputable certificate authority can still be infected with malware, or have other vulnerabilities with their Web infrastructure.

**What it means for consumers:** Consumers should look for SSL trust marks as a minimum standard of security when choosing what sites to shop with online. Providing credit card information, or other sensitive personal data to a Web merchant that does not encrypt with SSL, is like freeway driving without a seatbelt. But consumers should also know that the SSL trust mark is not a catchall security guarantee. The mark is a specific claim about the use of one particular type of security technology used to encrypt transactions, and it says nothing about other security or vulnerability aspects of an online merchant’s Web site.

**What it means for SMBs:** This trust mark is a must-have for small or medium businesses that want to run a technologically creditable e-commerce site. But an SSL trust mark should be considered the lowest common denominator in terms of security. SSL is a first-line defense against identity theft. Proving the use of SSL technology is the least a consumer-to-business or business-to-business site can do in terms of providing some security assurance to customers. Certainly more can be done, as we discuss later.

**Security/Vulnerability Scanning**

**What it is/what it does:** These marks denote that the online business uses a regularly scheduled security auditing and vulnerability detection service for its Web site, aimed at ensuring the site is free of malware, viruses, malicious downloads and other types of spyware. The audit also can include a check if the Web site’s code has vulnerabilities, which may not yet have been exploited by a hacker, but could be in the future. The detection service often uses proprietary tools, such as Web crawling and a scanning engine and a vulnerabilities database, to determine if a Web site is technically safe to visit form the standpoint of malware infection.

The McAfee SECURE service is one widely used comprehensive security/vulnerability scanning services that offers daily scanning and monitoring services for e-commerce Web sites. The vendor’s trust mark indicates that it is in compliance with the service’s requirements, which include passing a daily scan of its Web infrastructure for more than 10,000 vulnerabilities. In addition to this daily security testing, sites that earn the McAfee SECURE trust mark also undergo a series of reputation and behavioral tests that include checking for links to malicious Web sites, the hidden presence of browser exploit code and the sharing of customer e-mail data with spammers.

**Strengths and weaknesses:** The strength of vulnerability scanning can be illustrated by looking at the examples of Web site breaches discussed earlier. Privacy, reputation and SSL trust marks would not have helped any visitor to the compromised Web sites of Major League Baseball or Dolphins Stadium. However, if these sites had subjected themselves to a valid security/vulnerability scanning service and earned their seals, they would have identified and remediated the vulnerabilities, saving countless visitors from being at risk. As such, only a seal indicating a Web site has been externally scanned by a third-party security organization for vulnerabilities and malware infection can provide the extra level of assurance that a customer’s computer and personal information are protected from data- and identity-stealing malware infections.
Like the other trust marks examined, however, the security/vulnerability assessment seal is not a catchall for Internet security and safety either. In the parshilton.com example, the malware that was planted was a so-called zero-day type, about which antivirus vendors and security/vulnerability scanning providers had no knowledge or information. Vendors offering these types of scanning services can catch a lot of things. But in general, they cannot catch what they don't know about.

This is why scanning frequency is a critical metric to evaluate when considering a security/vulnerability scanning trust mark provider. In general, weekly scans are better than monthly scans and daily scans are better than weekly ones. Frequent scanning reduces the window of vulnerability to zero-day assaults (i.e., the parshilton.com example) and gives site administrators better information about their sites' weaknesses, which they can use to fix problems. In addition, trust mark providers that perform both signature- and behavior-based scans are, in general, better than ones that perform only one type of scan.

**What it means for consumers:** The security/vulnerability scanning trust mark denotes that a Web site is subjected to a thorough and regularly scheduled scan for vulnerabilities, which can result in the theft of consumer data loss or identities by hackers. This is different from soft trust marks (as in reputation and privacy marks), which typically put the onus on the Web merchant to abide by the rules the seal provider establishes. A regularly scanned Web site may also offer a higher degree of security for online shoppers than sites that display trust marks denoting the use of SSL certificates. However, consumers must be aware of the technical limitations of security/vulnerability scanning trust mark services (i.e., the zero-day issue mentioned above). Also, consumers should keep in mind that most security/vulnerability seals do not necessarily imply any compliance with the “soft” aspects of online trust like privacy policies or business reputation.

**What it means for SMBs:** A security/vulnerability scanning trust mark gives SMBs a high level of assurance that their site will not be compromised and used by hackers as a vehicle to infect visitors’ PCs or steal customers’ identities. This trust mark on an SMB’s e-commerce site can also differentiate the business from its same-sized competitors, who may also be turning to online selling and e-commerce. An SMB that displays and promotes a security/vulnerability scanning trust mark may have a competitive advantage over other SMB sites or larger brand name sites, selling similar products, but with lesser security guarantees. The mark also shows that the SMB is aware of the current online fraud/identity theft environment, and that protecting customers’ identities from theft or abuse is a priority.

**III. Conclusions and Recommendations**

The Internet is a more dangerous place than ever, as organized cybercriminals focus on identity theft as a source of revenue. Trust marks can go a long way toward making e-commerce less stressful for consumers. Consumers who restrict themselves to using sites with valid and effective trust marks cannot just reduce stress, but increase their security and reduce their likelihood of identity theft. SMBs can benefit in two ways by displaying trust seals that show they’ve taken measures to protect customers’ identities. Such seals can be both an effective marketing tool as well as just good Web security practice. To that end, Yankee Group recommends six ways consumers and SMBs can become more knowledge about what trust marks mean, and how they should be used.

**Recommendations**

The top six things consumers and SMBs should know about trust marks are as follows.

- **Don’t trust; verify.** Any consumer’s first approach to dealing with a Web site displaying a trust seal should be to click on the seal itself. Any Web site can simply copy and paste a GIF file of a reputable trust mark provider in an attempt to enhance its own appearance of security. A reputable trust mark provider will have a live link attached to its trust mark icon, which should take visitors to a verification Web site of the trust mark provider. In such cases, check the wording of the URL of the link, or type in the addresses of the seal provider into a Web browser and compare that to the suspicious site. Inquiring with the seal provider directly about a site displaying its logo is also a good measure to take.
• **Not all trust marks are the same.** Trust seals that provide a “set it and forget it” approach are of little use to both SMBs and their customers. Regarding soft trust marks—privacy and reputation—look for provider programs that offer regular audits of the measures and regulations they require of Web merchants displaying the logo. Hard trust mark programs should have regular update checks as well. In the best-case scenario, daily scanning and audits of a merchant’s Web site infrastructure can ensure the highest level security and safety.

• **No single trust mark covers everything.** There is no universal protection seal program. If consumers have multiple concerns about online shopping—wondering “Will this business keep my data safe?” and “Is this site technically safe?”—they should look for multiple seals. Some seal programs do cover multiple aspects of the four major areas. (For instance, BBBOnline has both reputation and privacy; the McAfee SECURE service scans for SSL, covers daily vulnerability scans as well as conducts reputation and behavioral tests.) If privacy is the top concern, then that trust mark may be the most important. If there is fear about the vulnerability of a Web site’s infrastructure, then a security/vulnerability scanning logo is paramount.

• **Read the fine print.** Both consumers and SMBs must know that logos or seals promising to keep data private should not be taken at face value. An organization may display the trust mark of a program, which requires them to post a privacy policy or give an opt-out option for personal data collection. However, it is up to consumers to go a step further and actually inspect exactly what the Web merchant’s policies and procedures look like. Also, look for trust mark programs that give consumers some recourse in terms of third-party mediation or complaint handling. This is important to customers if they fear their personal information may be misused, or if they’re concerned a merchant might not be acting in good faith. SMBs that belong to such trust mark programs can also provide customers with a level of reassurance that their worries won’t go unaddressed or unheard.

• **Trust marks can help improve business.** A trust seal is not just a piece of Internet eye candy or a hollow posture about security; consumers believe they work. As the Consumer Reports study indicated, 71 percent of consumers said they looked for these seals before doing online business with a merchant’s Web site. Competition for Web customers is about to get very hot for SMBs, with 33 percent currently using e-commerce now, and another 26 percent about to come online this year. An SMB showing a trust mark that demonstrates the use of strong security technology and identity-theft defense measures will stand out among the throng of small businesses that will be setting up Web shops soon.

• **Realize what online shoppers fear most.** Identity theft is the greatest fear facing online shoppers. Through media reports and personal experience, consumers are increasingly aware that a malware infection can lead to identity theft and data loss. SMBs who know this can help relieve this e-commerce angst by choosing trust marks that prove that their Web sites undergo the most rigorous security testing and auditing procedures.
Yankee Group—the global connectivity experts

The people of Yankee Group are the global connectivity experts™—the leading source of insight and counsel trusted by builders, operators and users of connectivity solutions for nearly 40 years. We are uniquely focused on the evolution of Anywhere, and chart the pace of technology change and its effect on networks, consumers and enterprises. For more information, visit http://www.yankeegroup.com/.

Yankee Group has research and sales staff located in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific. For more information, please contact one of the sales offices listed below.

Link Research
Yankee Group’s qualitative research forms the core of our offerings, with analysis focused exclusively on the transformational effects of the connectivity revolution. Our research reports arm you with the insight and analysis to make the right decisions today and tomorrow.

Link Data
Yankee Group’s quantitative data analysis includes monitors, surveys and forecasts. Together with Link Research, our data connects you to the information you need to make the most informed strategic and tactical business decisions.

Link Interaction
Connect one-on-one with Yankee Group analysts to get answers to your most strategic and critical questions, as well as gain deeper insight into research and trends. We encourage you to have direction interaction with analysts through ongoing conversations, conference calls and briefings.

Link Consulting
Who better than Yankee Group to help you define key global connectivity strategies, scope major technology initiatives and determine your organization’s readiness to undertake them, differentiate yourself competitively or guide initiatives around connectivity change? Our analysts apply Yankee Group research, methodologies, critical thinking and data to produce expert, timely, actionable results.

Link Events
The Anywhere revolution won’t wait. Join our live debates to discuss the impact that ubiquitous connectivity will have on your future. Yankee Group’s events—live and online—offer our clients new insight, knowledge and expertise to better understand and overcome the obstacles to succeed in this Anywhere revolution.