PE 3/25/2013

13001521

NO ACT

UNITED STATES
SECURITIES AND EXCHANGE COMMISSION
WASHINGTON, D.C. 20549

Received SEC

MAR 25 2013

Washington, DC 20549

DIVISION OF
CORPORATION FINANCE

March 25, 2013

Ronald O. Mueller
Gibson, Dunn & Crutcher LLP
shareholderproposals@gibsondunn.com

Act: 1934
Section:
Rule: 14a-8
Public
Availability: 3-25-13

Re: Amazon.com, Inc.

Dear Mr. Mueller:

This is in regard to your letter dated March 22, 2013 concerning the shareholder proposal submitted by the Pax World Mutual Funds for inclusion in Amazon.com's proxy materials for its upcoming annual meeting of security holders. Your letter indicates that the proponent has withdrawn the proposal and that Amazon.com therefore withdraws its January 22, 2013 request for a no-action letter from the Division. Because the matter is now moot, we will have no further comment.

Copies of all of the correspondence related to this matter will be made available on our website at http://www.sec.gov/divisions/corpfin/cf-noaction/14a-8.shtml. For your reference, a brief discussion of the Division's informal procedures regarding shareholder proposals is also available at the same website address.

Sincerely,

Erin E. Martin
Attorney-Advisor

cc: Joseph K. Keefe
Pax World Mutual Funds
30 Penhallow Street, Suite 400
Portsmouth, NH 03801

# GIBSON DUNN

Gibson, Dunn & Crutcher LLP

1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Tel 202.955.8500
www.gibsondunn.com

Ronald O. Mueller
Direct: +1 202.955.8671
Fax: +1 202.530.9569
RMueller@gibsondunn.com

March 22, 2013

VIA E-MAIL

Office of Chief Counsel
Division of Corporation Finance
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: *Amazon.com, Inc.*
*Shareholder Proposal of Pax World Mutual Funds*
*Securities Exchange Act of 1934—Rule 14a-8*

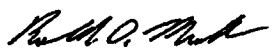
Ladies and Gentlemen:

In a letter dated January 22, 2013, we requested that the staff of the Division of Corporation Finance concur that our client, Amazon.com, Inc. (the "Company"), could exclude from its proxy statement and form of proxy for its 2013 Annual Meeting of Shareholders a shareholder proposal (the "Proposal") and statement in support thereof submitted by Pax World Mutual Funds (the "Proponent").

Enclosed as Exhibit A is a letter from the Proponent, dated March 22, 2013, withdrawing the Proposal. In reliance on the letter from the Proponent, we hereby withdraw the January 22, 2013 no-action request relating to the Company's ability to exclude the Proposal pursuant to Rule 14a-8 under the Securities Exchange Act of 1934.

Please do not hesitate to call me at (202) 955-8671 or Sarah Dods, the Company's Senior Corporate Counsel, at (206) 266-3192.

Sincerely,



Ronald O. Mueller

Enclosure

cc: Sarah Dods, Amazon.com, Inc.
Joseph F. Keefe, Pax World Mutual Funds
Corey Johnson, Pax World Mutual Funds
Sanford Lewis, Esq.

101483662.2

GIBSON DUNN

**EXHIBIT A**

March 22, 2013

David A. Zapolsky
Vice President, General Counsel and Secretary
Amazon.com, Inc.
410 Terry Avenue North
Seattle, WA 98109

Dear Mr. Zaplosky:

Pursuant to our correspondence on March 22, 2013, Pax World Mutual Funds (Pax World) hereby withdraws our shareholder proposal filed on December 7, 2012, entitled "Privacy and Data Security," for consideration at the 2013 annual shareholder meeting. This letter hereby acknowledges that Pax World formally withdraws our request to have our resolution presented on the 2013 Proxy Statement and be put to a vote by shareholders of the company.

Pax World, on behalf of our investors, wishes to thank Amazon.com and its Board of Directors for discussing our proposal in earnest and taking steps to enhance the company's public disclosure with respect to privacy and data security.

Sincerely,

Joseph F. Keefe
*President & CEO*
Pax World Mutual Funds

cc: Ronald O. Mueller, Gibson, Dunn & Crutcher LLP

# SANFORD J. LEWIS, ATTORNEY

March 6, 2013

Office of Chief Counsel
Division of Corporation Finance
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, D.C. 20549

Re: Shareholder proposal to Amazon.com, Inc. regarding oversight of privacy and data security – Proponent Response

Via email to shareholderproposals@sec.gov

Ladies and Gentlemen:

Pax World Mutual Funds ("Proponent") has submitted a shareholder proposal (the "Proposal") to Amazon.com, Inc. ("Amazon" or "Company") seeking a report on board of directors' oversight of privacy and data security. I have been asked by the Proponent to respond to the No Action request letter dated January 22, 2013, sent to the Securities and Exchange Commission by Ronald O. Mueller of the law firm of Gibson Dunn & Crutcher LLP on behalf of the Company. In that letter, the Company contends that the Proposal may be excluded from its 2013 proxy statement by virtue of Rule 14a-8(i)(7). A copy of this letter is being e-mailed concurrently to Ronald Mueller.

## SUMMARY

The Proposal, the full text of which is attached as Appendix A, requests:

> that the Board of Directors publish a report, at reasonable expense and excluding confidential or proprietary information, explaining how the Board is overseeing privacy and data security risks.

The Supporting Statement clarifies:

> We emphasize that the Proposal is not asking the Company to disclose risks, specific incidents, or legal compliance procedures; rather, we believe, investors need to understand more fully how the Board oversees the concerns described above.

The Company asserts that the Proposal is excludable pursuant to Rule 14a-8(i)(7), as addressing the Company's ordinary business -- the policing of privacy and data security. Although prior Staff decisions have allowed similar exclusions, this Proposal addresses a transcendent social policy issue. Amazon has become one of the most important controllers of the digital economy, both in its retail operations and as the economy's largest cloud computing provider. Accordingly, in this instance, the issue of board oversight of privacy and data, and the catastrophic risks associated with a failure of such oversight, is a very significant social policy issue, with

PO Box 231 Amherst, MA 01004-0231 • sanfordlewis@strategiccounsel.net
413 549-7333 ph. • 781 207-7895 fax

implications for the entire US and global economy. Therefore, the Proposal addresses a transcendent social policy issue with a clear nexus to the Company. Further, as an inquiry into the Company's oversight process, the Proposal does not micromanage. Accordingly, it is not excludable pursuant to Rule 14a-8(i)(7).

## BACKGROUND

In February 2013, President Obama declared that the "cyber threat is one of the most serious economic and national security challenges we face as a nation" and that "America's economic prosperity in the 21st century will depend on cybersecurity."[1]

Digital technologies and the Internet offer enormous opportunities, but as they have become embedded in nearly every aspect of our lives, they also carry substantial risk to our society as a whole, and to each of us that participates in the digital economy.

The Securities and Exchange Commission Division of Corporation Finance recognized the importance and arrival of this issue in 2011 with cybersecurity disclosure guidance. The guidance noted in its preamble:

> In general, cyber incidents can result from deliberate attacks or unintentional events. We have observed an increased level of attention focused on cyber attacks that include, but are not limited to, gaining unauthorized access to digital systems for purposes of misappropriating assets or sensitive information, corrupting data, or causing operational disruption. Cyber attacks may also be carried out in a manner that does not require gaining unauthorized access, such as by causing denial-of-service attacks on websites. Cyber attacks may be carried out by third parties or insiders using techniques that range from highly sophisticated efforts to electronically circumvent network security or overwhelm websites to more traditional intelligence gathering and social engineering aimed at obtaining information necessary to gain access.
>
> The objectives of cyber attacks vary widely and may include theft of financial assets, intellectual property, or other sensitive information belonging to registrants, their customers, or other business partners. Cyber attacks may also be directed at disrupting the operations of registrants or their business partners.[2]

Others have noted that cyber security is not just a risk to individual companies, it also places our economy at risk.[3] Amazon, which has positioned itself at the pinnacle of the digital economy, could prove to be a linchpin and vulnerable point in our entire economic structure. Because its cloud computing business is relied upon heavily by both government and commercial operations throughout the economy, a failure of privacy and data security by Amazon could have

---

[1] http://www.whitehouse.gov/cybersecurity
[2] CF Disclosure Guidance: Topic No. 2 , Cybersecurity, October 13, 2011.
[3] http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

catastrophic implications. Not only is the economic well-being and privacy of its customers at risk, but so is trust in, and infrastructure of, the digital economy

A front page New York Times story ("As Hacking Against U.S. Rises, Experts Try to Pin Down Motive"[4]) reported that "corporate America is caught between what it sees as two different nightmares – preventing a crippling attack that brings down America's most critical systems, and preventing Congress from mandating that the private sector spend billions of dollars protecting against the risk."

What's clear is that privacy and data security are, and will continue to be, critical and consistent issues of public policy debate for many years to come. As one corporate lawyer wrote about the role of the Board of Directors in overseeing these issues:

> The issue of cybersecurity risk is likely to grow in prominence as our society and economy become ever more dependent on technology. Likewise, effective corporate management of cybersecurity is increasingly important not only for a company's employees, customers, and business partners, but also for society at large. As U.S. Cyber Security Coordinator Schmidt noted, "Until such time as cybersecurity becomes a regular board of directors' agenda item and measurable progress [is] made consistent with International Information Security standards ..., the potential for disruption is real and serious and we all pay the price."[5]

Investors have every reason to be concerned and involved about privacy and data security – not on a day-to-day operational level, but by seeking to ensure that Amazon's Board is adequately addressing the risks these issues present both to the Company and society. Yet, it is unclear to investors how the Company's board of directors is overseeing the relevant risks and heading off such a potentially catastrophic outcome for the Company and the US and global economies. Thus, the current Proposal seeks to create transparency regarding that oversight process.

## ANALYSIS

**The Proposal addresses a significant social policy issue that transcends ordinary business.**

The Company accurately notes that prior Staff decisions have found proposals relating to data security and privacy to be excludable as ordinary business, pursuant to Rule 14a-8(i)(7). The current proposal stands in distinction from those proposals, because the Company's management of these issues is not a simple internal matter but rather can jeopardize the fate of the US and global economy. Therefore, in the instance of this company, this is a significant policy issue that transcends ordinary business.

Under the Staff's decision-making process, an issue may not be considered a significant policy

---

[4] http://www.nytimes.com/2013/03/04/us/us-weighs-risks-and-motives-of-hacking-by-china-or-iran.html?hpw
[5] http://blogs.law.harvard.edu/corpgov/2012/12/16/cybersecurity-risks-and-the-board-of-directors/

issue one year, but can rise to such a status if the issue has congressional, public and media attention, and a clear nexus to the company. This has happened in recent years on various other issues including net neutrality, antibiotics in animal feed and climate change. With this proposal, we believe the Staff should make the same determination regarding privacy and data security at Amazon.

**The Nexus to Amazon.com**

Amazon, which began in 1995 as an online book store, has since grown into the world's largest online retailer.

Amazon now also offers a variety of entertainment media, manufacturing and selling Kindle tablet devices as well as online music and video. By some estimates, the company's sites are viewed by more than 100 million different people in the U.S. every month.[6]

However, Amazon is also the largest provider of cloud computing. Amazon's AWS unit is the undisputed leader in the world's cloud computing business, with an estimated 70 percent market share, according to one analyst. AWS revenue has grown from an estimated $500 million in 2010 to an estimated $1.5 billion in 2012.[7] According to one report (based on data provided by Amazon), as the third quarter (2012) came to a close, AWS had 1.3 trillion objects stored in its S3 (simple storage) service, and it was fielding 835,000 requests per second for objects under peak loads.[8]

Amazon's cloud computing customers include businesses and government agencies (such as NASDAQ and the U.S. Treasury). As such, the Company now plays a pivotal role in the U.S. and world economies. These customers entrust Amazon with huge amounts of data, much of it confidential information about *their* customers.[9]

---

[6] http://www.wired.com/business/2012/10/amazon-next-advertising-giant/

[7] http://tech.fortune.cnn.com/2012/05/22/aws/

[8] http://www.theregister.co.uk/2012/11/29/amazon_aws_update_jassy/

[9] ***Amazon's AWS Unit***

**In announcing its cybersecurity initiative[9], the Obama administration noted that the "U.S. Government depends on a variety of privately owned and operated critical infrastructures to carry out the public's business. In turn, these critical infrastructures rely on the efficient operation of information systems and networks that are vulnerable to malicious cyber threats. In fact, according to the Company, Amazon's AWS unit provides vital cloud computing services to over 300 government agencies including the U.S. Department of the Treasury, U.S. Department of State, U.S. Department of Agriculture, NASA Jet Propulsion Lab, and the U.S. Army, Navy, Air Force, and Marine Corps.**

**AWS's for-profit clients, according to the Company, include NASDQ, Thomson Reuters, Ericsson, Pfizer, Unilever, Harvard Medical School, NYU Langone Medical Center, News International, Guardian News and Media, PBS, NetFlix, Pinterest, Airbnb, and Obama for America.[9] By one account, Amazon's AWS unit has more than 60,000 clients, including divisions of large banks and pharmaceutical companies.**

**These clients use AWS for a variety of services, and in almost all cases they are using Amazon to store, generate or distribute highly-confidential data. As explained on Amazon's web site, for example:**

- **NASDAQ "uses Amazon Web Services (AWS) as the basis for FinQloud, a cloud computing solution specific to the financial services industry. FinQloud enables clients to store, manage and process large amounts of data cost-effectively while also helping them meet regulatory requirements."**

**A failure of Amazon to oversee data privacy and security could "disrupt" the US economy.**

Amazon's role has often been characterized as "disruptive" of existing business models. But as the great digital disruptor of economic models, it has become a steward of a vital portion of the economy's commercial plumbing. The disruption that it could impose on the rest of us in the event of a catastrophic failure in privacy or security is one of the looming issues of our time.

The media have taken notice. The *Financial Times* observed in 2012[10]:

> Amazon has long thrived by overturning the way people shop, but its shift into infrastructure is extending its power as a disruptive force to how business is structured. It is revolutionising the way entrepreneurs can create start ups, or revive staid companies, by letting them plug their ideas into pay-as-you-go systems that cost a fraction of the investment they would need to build such infrastructure alone.
>
> This has lifted Amazon's economic influence beyond its tech peers Apple, Google and Facebook and taken it into the realm of network businesses such as stock exchanges, power grid operators, credit card processors and shipping lines.
>
> But its emergence as a new and largely unregulated steward of such vital commercial plumbing creates tensions and dangers for clients and parts of the US economy.

**The Public Debate**

Privacy and data security have become the focus of national and international discussion and debate, addressed as top-level priorities by heads-of-government and legislatures around the world. They are also the focus of national and international lobbying campaigns (including by Amazon), investigation by numerous non-governmental organizations, and an extraordinary amount of media attention.

In announcing support of Data Privacy Day 2013, Sen. Patrick Leahy said[11]:

> I join privacy advocates, industry leaders and National, State and local government officials from across our Nation in celebrating Data Privacy Day--a day to recognize the

---

- Pfizer "has set up an instance of the Amazon Virtual Private Cloud (Amazon VPC) to provide a secure environment in which to carry out computations for worldwide research and development (WRD), which supports large-scale data analysis, research projects, clinical analytics, and modeling."
- Obama for America "designed, built, and deployed an election-winning technology system by using Amazon Web Services (AWS). The campaign technology team built close to 200 applications that kept thousands of volunteers connected and collaborating across the United States."

[10] http://www.ft.com/cms/s/0/cc3a0eee-c1de-11e1-8e7c-00144feabdc0.html#axzz2MJf8zyXb
[11] http://thomas.loc.gov/cgi-bin/query/z?r113:S28JA3-0020:

> need to better secure our privacy and security in cyberspace…In the Digital Age, Americans face new threats to their digital privacy and security as consumers and businesses alike collect, share and store more and more information in cyberspace.

Another important indicator of Congressional sentiment was the creation of a new Senate Judiciary Subcommittee on Privacy, Technology and the Law, effective at the start of the 112th Congress (January 2011). Sen. Al Franken, chairman of the subcommittee, has said he "plans to use his new position to try to strike a balance between the benefits of new technology and our fundamental right to privacy."

Sen. Franken said privacy and data security were critical to the future of the Internet:

> (E)very few weeks, we hear about yet another breach: Yahoo! and Gmail; Citibank; Bank of America; Sony PlayStation. Millions of people who have had their names, passwords, credit card information, or health information compromised. And it isn't just our national security or economic well-being that's being threatened by these attacks - it's the Internet itself. If you want to use Facebook or a cloud-based email provider to communicate with your friends and loved ones, you need to know that your private communications won't be exposed by hackers. If you want to use the Internet to spread new ideas or fight for democracy, you need to know that your work won't be disrupted by hackers or repressive regimes.

Sen. Franken on privacy: "Today, advanced technology has provided us an ever-increasing array of products and services. But it has also placed an incredible amount of our personal data into the hands of private companies-including many that consumers have never even heard of. Consumers are not aware of all the ways in which data can be collected about them: one recent survey found that the top 50 websites installed an average of 64 tracking devices on their visitors' computers. Often this information is sold and resold, making it impossible to know who has your personal data and what they might do with it."[12]

In September 2012, Sen. Jay Rockefeller, Chairman of the Senate Committee on Commerce, Science, and Transportation, sent letters to every CEO of *Fortune's* top 500 companies — including Amazon CEO Jeff Bezos — asking them to outline what measures their companies have in place to protect their computer systems from cyberattacks.[13] On Feb. 28, 2013, Sen. Rockefeller and Sen. Tom Carper, chairman of the Homeland Security Committee, announced that they would soon hold joint hearings on cybersecurity.

Sen. Rockefeller's interest in cybersecurity has been mirrored by the actions of other legislators. For example, Senator John Kerry, former Chairman of the Commerce Subcommittee on Communications, Technology, and the Internet (and now Secretary of State) and Sen. John McCain, former chairman of the Commerce Committee, proposed *The Commercial Privacy Bill*

---

[12] http://www.franken.senate.gov/?p=issue&id=297
[13] http://thehill.com/blogs/hillicon-valley/technology/250335-rockefeller-asks-ceos-of-500-top-us-companies-for-views-on-cybersecurity#ixzz2MECMr4bu

*of Rights Act of 2011* that would have established a framework to protect the personal information of all Americans.[14] "Consumers want to shop, browse and share information in an environment that is respectful of their personal information. Our legislation sets forth a framework for companies to create such an environment and allows businesses to continue to market and advertise to all consumers, including potential customers," said Senator McCain.

**Expert analysis of public attention to this issue documents high level of interest and concern**

The late Alan F. Westin, Columbia University Professor Emeritus of Public Law and Government, and a world-recognized privacy expert, wrote in December 2012[15]:

> Privacy has become a central issue and fierce battleground of the technology-driven world we inhabit. To see how profoundly important this has become, we can go to a search engine and see how often privacy is mentioned in published materials of all kinds, including web pages...."Privacy" produces a staggering 11.930B results—almost twelve billion items—a stunning but trustworthy portrait of just how central privacy has become in the U.S. today.

As the Center for Democracy and Technology has observed[16]:

> Privacy is the number one concern of Internet users; it is also the top reason why non-users still avoid the Internet. Survey after survey indicates mounting concern. While privacy faces threats from both private and government intrusions, the existing motley patchwork of privacy laws and practices fails to provide comprehensive protection. Instead, it causes confusion that fuels a sense of distrust and skepticism, limiting realization of the Internet's potential.

This concern is reflected in the increasing attention given to privacy and data security (sometimes known as "cybersecurity") by governments, legislatures and regulators in the U.S. and abroad. Importantly, much of this attention conjoins *national policy interests* with calls to action for *companies* to develop and implement appropriate policies and practices.

**Obama Administration Initiatives**

In February 2012, for example, the Obama Administration unveiled a "Consumer Privacy Bill of Rights"[17] as part of a "comprehensive blueprint to protect individual privacy rights and give users more control over how their information is handled." The administration said the initiative

---

[14] http://www.kerry.senate.gov/press/release/?id=59a56001-5430-4b6d-b476-460040de027b
[15] https://www.privacyassociation.org/publications/2012_12_17_how_important_is_privacy_today
[16] https://www.cdt.org/issue/consumer-privacy
[17] http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-privacy-b

"seeks to protect all Americans from having their information misused by giving users new legal and technical tools to safeguard their privacy."

President Obama said[18]:

> **Never has privacy been more important than today, in the age of the Internet, the World Wide Web and smart phones.** In just the last decade, the Internet has enabled a renewal of direct political engagement by citizens around the globe and an explosion of commerce and innovation creating jobs of the future. Much of this innovation is enabled by novel uses of personal information. So, it is incumbent on us to do what we have done throughout history: apply our timeless privacy values to the new technologies and circumstances of our times.

In a related report (*Consumer Data Privacy in a Networked World*), the Administration said:

> **Privacy protections are critical to maintaining consumer trust in networked technologies.** When consumers provide information about themselves—whether it is in the context of an online social network that is open to public view or a transaction involving sensitive personal data—they reasonably expect companies to use this information in ways that are consistent with the surrounding context. Many companies live up to these expectations, but some do not. **Neither consumers nor companies have a clear set of ground rules to apply in the commercial arena. As a result, it is difficult today for consumers to assess whether a company's privacy practices warrant their trust.**

**An under-regulated issue generates calls for "enforceable codes of conduct"**

President Obama called on companies that use personal data "to begin immediately working with privacy advocates, consumer protection enforcement agencies, and others to implement these principles in enforceable codes of conduct." As part of that process, the Administration said the Commerce Department's National Telecommunications and Information Administration (NTIA) would convene Internet companies and consumer advocates to develop enforceable codes of conduct that comply with the Consumer Privacy Bill of Rights, building on strong enforcement by the Federal Trade Commission.

**Federal agency action demonstrates high-profile debate**

Privacy and data security have become increasing concerns of a number of U.S. government agencies. The Federal Trade Commission, for example, has led a multi-year initiative, including three wide-ranging workshops and two reports, to create a comprehensive framework for protecting privacy. In March 2012, the agency released a long-awaited report on consumer privacy, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for

[18] http://www.whitehouse.gov/sites/default/files/privacy-final.pdf

Businesses and Policymakers."[19]

The FTC said it received more than 450 public comments in response to the preliminary report from various stakeholders, including businesses, privacy advocates, technologists and individual consumers. "A wide range of stakeholders, including industry, supported the principles underlying the framework, and many companies said they were already following them. At the same time, many commenters criticized the slow pace of self-regulation, and argued that it is time for Congress to enact baseline privacy legislation," the FTC said.

In October 2011, the SEC's Division of Corporation Finance issued guidance[20] "regarding disclosure obligations relating to cybersecurity risks and cyber incidents." In issuing the guidance, CorpFin observed: "For a number of years, registrants have migrated toward increasing dependence on digital technologies to conduct their operations. As this dependence has increased, the risks to registrants associated with cybersecurity have also increased, resulting in more frequent and severe cyber incidents."

National and international policy discussions regarding privacy and data security have drawn the attention of Amazon management. In the U.S., Amazon joined with other companies in 2012 to form the Internet Association[21], a lobbying group whose stated mission includes activities related to privacy and data security.

In Brussels, the EU last year introduced a draft of a new EU data protection regulation which includes major changes to current law.[22]According to *The New York Times*, the new law "would force Internet companies like Amazon and Facebook to obtain explicit consent from consumers about the use of their personal data, delete that data forever at the consumer's request and face fines for failing to comply."

**Media coverage raises the visibility of the issue**

Privacy and data security are subjects of ongoing attention by the mainstream media as well as trade publications and online commentators.

As but one example, *The Wall Street Journal* has published an ongoing multi-year series, entitled "What They Know," exploring the issue of privacy.[23] Says the *Journal*: "The age of computing has created a new economy, in which data on people's habits, activities and interests is collected, sold and traded, often without their knowledge. The Wall Street Journal's What They Know series documents new, cutting edge uses of tracking technology and what the rise of ubiquitous surveillance means for consumers and society."

---

[19] http://www.ftc.gov/os/2012/03/120326privacyreport.pdf
[20] http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
[21] http://internetassociation.org/
[22] http://www.spiegel.de/international/europe/the-european-union-closes-in-on-data-privacy-legislation-a-877973.html
[23] http://online.wsj.com/public/page/what-they-know-digital-privacy.html

On one very recent day (March 4, 2013), *The New York Times* featured no less than three prominent stories regarding privacy and data security.

- A story on the front page of the Business Day section ("Web Privacy Becomes a Business Imperative"[24]) reported that "Privacy is no longer just a regulatory headache. Increasingly, Internet companies are pushing each other to prove to consumers that their data is safe and in their control."
- A front page story ("As Hacking Against U.S. Rises, Experts Try to Pin Down Motive"[25]) reported that "corporate America is caught between what it sees as two different nightmares – preventing a crippling attack that brings down America's most critical systems, and preventing Congress from mandating that the private sector spend billions of dollars protecting against the risk."
- And a third story ("Where Apps Meet Work, Secret Data is at Risk"[26]), specifically mentioned Amazon: "Some apps onto which employees may move company information, like Facebook and Amazon, are well known."

**Risks for Amazon**

Privacy and data security present very real potential risks for Amazon. That is why Proponents have requested that the Company's Board report on how it is managing those risks. For example, a recent assessment of strengths and weaknesses in privacy and data security among tech companies, conducted by the Electronic Frontier Foundation, concluded:

> Amazon is entrusted with huge quantities of information as part of its cloud computing services and retail operations, yet does not produce annual transparency reports, publish a law enforcement guide, or promise to inform users when their data is sought by the government.[27]

The recent history of privacy and security related litigation against Amazon evidences substantial vulnerabilities:

- Amazon's Zappos unit, an online shoe retailer, is the defendant in a consolidated class action lawsuit brought on behalf of some 24 million customers. The suit alleges that Amazon violated the Fair Credit Reporting Act in January 2012 when it allowed a hacker to access part of its internal network and systems, enabling the hacker to gain access to customer personal information such as names and addresses, email addresses, phone numbers, encrypted passwords, and the last four digits of credit card numbers. In addition to the lawsuit, the Attorneys General of nine states, including Connecticut Kentucky,

[24] http://bits.blogs.nytimes.com/2013/03/04/daily-report-web-privacy-becomes-a-business-imperative/
[25] http://www.nytimes.com/2013/03/04/us/us-weighs-risks-and-motives-of-hacking-by-china-or-iran.html?hpw
[26] http://www.nytimes.com/2013/03/04/technology/it-managers-struggle-to-contain-corporate-data-in-the-mobile-age.html?pagewanted=1
[27] https://www.eff.org/pages/who-has-your-back

Florida, Massachusetts, North Carolina, New York and Pennsylvania sent a letter to Amazon seeking additional information about the incident.[28]

- In November 2012, Amazon settled a class action lawsuit which alleged that the Company circumvented the privacy settings of Internet Explorer users. The lawsuit claimed that customers who used Microsoft's web browser, Internet Explorer, were essentially tricked into thinking the e-commerce site was "more privacy-protective than it actually is." The lawsuit further alleged Amazon used Flash cookies to collect users' personal information even if they had set their browser to block cookies. This information was then allegedly shared with other companies, without the consumer's permission, to send them targeted ads, the lawsuit stated. Terms of the settlement were not disclosed.[29]

- According to the Bloomberg news service, a hacker used Amazon's Elastic Computer Cloud service to attack Sony Corp.'s PlayStation Network online entertainment systems in April 2011, leading to the second-largest online data breach in U.S. history. The Bloomberg report noted: "The incident helps illustrate the dilemma facing Chief Executive Officer Jeff Bezos: Amazon's cloud-computing service is as cheap and convenient for hackers as it is for customers."[30]

**Amazon board member acknowledges national cyber security risks**

Jamie Gorelick, a partner of the law firm Wilmer Cutler Pickering Hale and Dorr LLP, is also a member of the Amazon board of directors[31] In July 2010, prior to joining Amazon's board, Ms. Gorelick was the featured speaker at a Washington, D.C. event of the organization, Women in Homeland Security. Ms. Gorelick discussed "gaps in the nation's cyber security."[32] In response to a question, she said: "I think that we need to rethink the relationship between the private sector and the public sector and make it more robust."

**The Proposal does not micromanage the Company**

The Proposal seeks top level information about how the Board is managing the issues of privacy and data security and their considerable risks to the Company. The current oversight of these issues at the company is unclear and insufficiently transparent, in the opinion of the Proponent. As stated in the supporting statement: We emphasize that the Proposal is not asking the Company to disclose risks, specific incidents, or legal compliance procedures; rather, we believe, investors need to understand more fully how the Board oversees the concerns described above.

---

[28] http://www.topclassactions.com/lawsuit-settlements/lawsuit-news/2633-zapposcom-loses-arbitration-bid-in-data-breach-class-action-lawsuit
[29] http://www.bigclassaction.com/settlement/amazon-flash-cookie-class-action-lawsuit-settlement.php
[30] http://www.bloomberg.com/news/2011-05-15/sony-attack-shows-amazon-s-cloud-service-lures-hackers-at-pennies-an-hour.html
[31] http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-govBio&ID=219511
[32] http://vimeo.com/12366652

The need for better transparency regarding the oversight process is clear. Proponent notes that the terms "privacy" and "data security" are not even mentioned in the charter of any of the company's Board committees: the Audit Committee, Nominating and Corporate Governance Committee, or the Leadership Development and Compensation Committee. Similarly, they are not mentioned in the Company's Corporate Governance Guidelines or its Code of Business Conduct and Ethics.

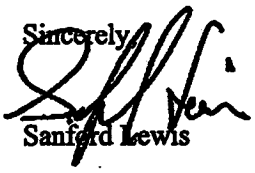
As demonstrated above, the issues of privacy and data security have been the subject of widespread public debate, media coverage, regulatory activity, and legislative activity for many years, and the debate shows no signs of subsiding. It will continue in court, in Congress, at the FTC, in academia, in the newspapers and online. It is a hugely significant public policy issue confronting the Company right now and for that reason it is appropriate for shareholder consideration.

## CONCLUSION

As demonstrated above, Proponent urges the Staff to find that the Proposal addresses a significant policy issue, does not micromanage, and has a clear nexus to the Company, and thus the Proposal is not excludable under Rule 14a-8(i)(7).

Please call me at (413) 549-7333 with respect to any questions in connection with this matter, or if the Staff wishes any further information.

Sincerely,



Sanford Lewis

cc:

Pax World Mutual Funds
Ronald O. Mueller

**EXHIBIT A**
**THE PROPOSAL**

**Privacy and Data Security**

Whereas,

As a leader in online retailing, entertainment media, and cloud computing services to businesses, Amazon.com ("Amazon") confronts serious privacy and data security risks.

Breaches of privacy and data security are a growing threat which can result from company negligence or external attacks. Cyberattacks on U.S. computer networks rose 17-fold from 2009 to 2011, according to the National Security Agency.[i]

According to a 2011 Ponemon Institute study, the per capita cost of a data breach was $194, with an average incident cost of $5.5 million.[ii] A separate Ponemon study found data breaches could negatively impact brand value and reputation by as much as 12 percent to 25 percent, with the average loss in brand value ranging from $184 million to more than $330 million.[iii]

Unauthorized collection, disclosure, or misuse of personal information can cause great harm to individuals and society - including discrimination, identity theft, financial loss, loss of business or employment opportunities, humiliation, reputational damage, questionable government surveillance, or physical harm.

The Electronic Frontier Foundation said in a 2012 report[iv]: "Amazon is entrusted with huge quantities of information as part of its cloud computing services and retail operations, yet does not produce annual transparency reports, publish a law enforcement guide, or promise to inform users when their data is sought by the government."

In 2012 Amazon's Zappos unit and an affiliated site were the victims of a data breach which exposed personal information of more than 24 million customers, resulting in a consolidated class action lawsuit.[v] The New York Times observed: "The breaches at Amazon's sites, combined with several recent cyberattacks, could threaten to shake consumer confidence online."[vi]

We believe Amazon's Board has a fiduciary and social responsibility to protect company assets, including the personal information of a variety of stakeholders.

**Resolved,** that the Board of Directors publish a report, at reasonable expense and excluding confidential or proprietary information, explaining how the Board is overseeing privacy and data security risks.

**Supporting Statement**

We emphasize that the Proposal is not asking the Company to disclose risks, specific incidents, or legal compliance procedures; rather, we believe, investors need to understand more fully how the Board oversees the concerns described above.

Carnegie Mellon University's Cylab published a 2012 report ("How Boards and Senior Executives Are Managing Cyber Risks"[vii]) which we believe could be instructional in writing this report. Among Cylab's recommendations for boards:

"Review existing top-level policies to create a culture of security and respect for privacy. Organizations can enhance their reputation by valuing cyber security and the protection of privacy and viewing it as a corporate social responsibility."

"Review assessments of the organization's security program and ensure that it comports with best practices and standards and includes incident response, breach notification, disaster recovery, and crisis communications plans."
"Conduct an annual review of the enterprise security program and effectiveness of controls, to be reviewed by the board Risk Committee, and ensure that identified gaps or weaknesses are addressed."

---

[i] http://www.bloomberg.com/news/2012-08-29/sec-guidance-on-cyber-disclosure-becomes-rule-for-google.html

[ii] http://www.cbiz.com/ras/pdfs/2011_Ponemon_Study.pdf

[iii] http://www.worldnews.se/news/60845/new-survey-by-the-ponemon-institute-finds-that-data-breaches-can-cause-lasting-a/

[iv] https://www.eff.org/pages/who-has-your-back

[v] http://www.topclassactions.com/lawsuit-settlements/lawsuit-news/1575-zappos-hack-leads-to-class-action-lawsuit

[vi] http://bits.blogs.nytimes.com/2012/01/17/even-big-companies-cannot-protect-their-data/

[vii] http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf

GIBSON DUNN

Gibson, Dunn & Crutcher LLP

1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Tel 202.955.8500
www.gibsondunn.com

Ronald Mueller
Direct: 202.955.8671
Fax: 202.530.9569
RMueller@gibsondunn.com

January 22, 2013

VIA E-MAIL

Office of Chief Counsel
Division of Corporation Finance
Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549

Re: *Amazon.com, Inc.*
*Shareholder Proposal of Pax World Mutual Funds*
*Securities Exchange Act of 1934—Rule 14a-8*

Ladies and Gentlemen:

This letter is to inform you that our client, Amazon.com, Inc. (the "Company"), intends to omit from its proxy statement and form of proxy for its 2013 Annual Meeting of Shareholders (collectively, the "2013 Proxy Materials") a shareholder proposal (the "Proposal") and statements in support thereof received from Pax World Mutual Funds (the "Proponent").

Pursuant to Rule 14a-8(j), we have:

- filed this letter with the Securities and Exchange Commission (the "Commission") no later than eighty (80) calendar days before the Company intends to file its definitive 2013 Proxy Materials with the Commission; and

- concurrently sent copies of this correspondence to the Proponent.

Rule 14a-8(k) and Staff Legal Bulletin No. 14D (Nov. 7, 2008) ("SLB 14D") provide that shareholder proponents are required to send companies a copy of any correspondence that the proponents elect to submit to the Commission or the staff of the Division of Corporation Finance (the "Staff"). Accordingly, we are taking this opportunity to inform the Proponent that if the Proponent elects to submit additional correspondence to the Commission or the Staff with respect to this Proposal, a copy of that correspondence should be furnished concurrently to the undersigned on behalf of the Company pursuant to Rule 14a-8(k) and SLB 14D.

## THE PROPOSAL

The Proposal states:

> **Resolved**, that the Board of Directors publish a report, at reasonable expense and excluding confidential or proprietary information, explaining how the Board is overseeing privacy and data security risks.

A copy of the Proposal, as well as related correspondence with the Proponent, is attached to this letter as Exhibit A.[1]

## BASIS FOR EXCLUSION

We hereby respectfully request that the Staff concur in our view that the Proposal may be excluded from the 2013 Proxy Materials pursuant to Rule 14a-8(i)(7) because the Proposal relates to the Company's ordinary business operations.

## ANALYSIS

**The Proposal May Be Excluded Under Rule 14a-8(i)(7) Because The Proposal Pertains To Matters Of The Company's Ordinary Business Operations And Does Not Raise A Significant Policy Issue.**

The Proposal properly may be omitted pursuant to Rule 14a-8(i)(7) because it deals with protection of electronically stored information and privacy, including the privacy of the Company's customers, which are matters relating to the Company's ordinary business operations. Rule 14a-8(i)(7) permits the omission of shareholder proposals dealing with matters relating to a company's "ordinary business" operations. According to the Commission release accompanying the 1998 amendments to Rule 14a-8, the underlying policy of the ordinary business exclusion is "to confine the resolution of ordinary business problems to management and the board of directors, since it is impracticable for shareholders to decide how to solve such problems at an annual shareholders meeting." Exchange Act Release No. 40018 (May 21, 1998) (the "1998 Release"). In the 1998 Release, the

---

[1] As reflected in Exhibit A, the Proposal is a revised version of a proposal that the Company initially received on December 10, 2012. The revisions were pursuant to a deficiency notice that the Company sent to the Proponent regarding the 500-word limit in Rule 14a-8(d).

Commission further explained that the term "ordinary business" refers to matters that are not necessarily "ordinary" in the common meaning of the word, but that the term "is rooted in the corporate law concept [of] providing management with flexibility in directing certain core matters involving the company's business and operations." In the 1998 Release, the Commission explained that the ordinary business exclusion rests on two central considerations. As relevant here, one of these considerations is that "[c]ertain tasks are so fundamental to management's ability to run a company on a day-to-day basis that they could not, as a practical matter, be subject to direct shareholder oversight." *Id.*

A proposal being framed in the form of a request for a report does not change the nature of the proposal. The Commission has stated that a proposal requesting the dissemination of a report may be excludable under Rule 14a-8(i)(7) if the subject matter of the report is within the ordinary business of the issuer. *See* Exchange Act Release No. 20091 (Aug. 16, 1983).

The Proposal requests a report on "how the Board is overseeing privacy and data security risks." The Proposal's request for an explanation of the Board's oversight of certain risks does not preclude exclusion if the underlying subject matter of the Proposal is ordinary business. The Staff indicated in Legal Bulletin No. 14E (Oct. 27, 2009) ("SLB 14E") that, in evaluating shareholder proposals that request a risk assessment, it bases its analysis under Rule 14a-8(i)(7) on "whether the underlying subject matter of the risk evaluation involves a matter of ordinary business to the company," and in analyzing shareholder proposals relating to the board's oversight of particular risks, the Staff has similarly looked to the underlying subject matter of the risk(s) and has concurred in the exclusion of a proposal when that underlying subject matter has involved a matter of ordinary business to the company. For example, in *Sempra Energy* (avail. Jan. 12, 2012, *recon. denied* Jan. 23, 2012), the proposal urged the board "to conduct an independent oversight review of the [c]ompany's management of political, legal, and financial risks posed by Sempra operations in any country that may pose an elevated risk of corrupt practices." Notwithstanding the proponent's argument that the "Staff recognized in SLB 14E that shareholders have an especially keen interest in the board of directors' role in the oversight of a company's management of risk," the Staff concurred that the proposal could be excluded pursuant to Rule 14a-8(i)(7). The Staff noted in its response letter that "although the proposal requests the board to conduct an independent oversight review of Sempra's management of particular risks, the underlying subject matter of these risks appears to involve ordinary business matters." Likewise, in *The Western Union Co.* (avail. Mar. 14, 2011), the Staff considered a proposal that requested the company to establish a risk committee on its board of directors and to report on certain identified risk categories. In concurring that the proposal properly could be excluded under Rule 14a-8(i)(7), the Staff in particular noted that the proposal "requests a report that describes how Western Union monitors and controls particular risks." *See also Wells Fargo & Co. (Recon.)* (avail. Apr. 5, 2011) (affirming the excludability of a

proposal seeking a report on the board's "actions to ensure that employee compensation does not lead to excessive and unnecessary risk-taking that may jeopardize the sustainability of the [c]ompany's operations" when one of the specified subjects of the report addressed employee compensation, a matter of ordinary business). As with the foregoing precedent, the Proposal as discussed below addresses particular business risks and relates to a subject matter that constitutes ordinary business operations for the Company, specifically, "privacy and data security risks."

The Staff consistently has concurred that proposals regarding procedures for protecting customer information and privacy, including Internet privacy, are excludable as relating to a company's ordinary business. For instance, in *Bank of America Corp.* (avail. Feb. 21, 2006) ("*Bank of America 2006*"), the proposal requested a report on Bank of America's "policies and procedures for ensuring that all personal and private information pertaining to all Bank of America customers will remain confidential in all business operations." The company argued that the proposal was excludable because it concerned a core management function and attempted to "usurp[] management's authority by allowing stockholders to govern the day-to-day business of managing the banking and financial relationships that [Bank of America] has with its customers and the privacy protection afforded to its customers." The Staff concurred with the proposal's exclusion under Rule 14a-8(i)(7), noting that the proposal related to the company's ordinary business operations, specifically the "procedures for protecting customer information." Similarly, in a recent no-action letter, a proposal requested that a company "adopt a minimum seven-year records retention policy (or longer, depending upon applicable laws) on all electronic loan files, and adopt necessary internal controls to safeguard these assets from unauthorized access and accidental loss or deletion." In concurring with exclusion of the proposal under Rule 14a-8(i)(7), the Staff noted that the proposal "relates to the policies and procedures for the retention of records regarding the products and services [the company] offers." *Huntington Bancshares Inc.* (avail. Jan. 10, 2011). In *Comcast Corp.* (avail. Mar. 4, 2009), the Staff concurred with the exclusion of a proposal requesting a report on "the effects of the company's Internet network management practices in the context of the significant public policy concerns regarding the public's expectations of privacy . . . on the Internet," noting that the proposal related to the ordinary business matter of "procedures for protecting user information." *See also Qwest Communication International Inc.* (Feb. 17, 2009) (same); *Verizon Communications Inc.* (avail. Feb. 13, 2009) (same); *AT&T Inc.* (avail. Jan. 26, 2009, *recon. denied* Feb. 27, 2009) (same).

Similarly, in *Consolidated Edison, Inc.* (avail. Mar. 10, 2003), the Staff concurred that a proposal requesting new procedures for protecting customer privacy was excludable as relating to the Company's ordinary business. The proposal submitted to Consolidated Edison requested that company employees that enter customers' homes to service electric

systems and read electrical meters "not . . . concern themselves with and/or report to others including any governmental agency, lifestyles as may be evidenced by, for example, garments, reading material, or other paraphernalia related to any religion or belief of any organization or group, as to, the occupants of the premises." The Staff concurred that the proposal was excludable under Rule 14a-8(i)(7) because it related to the "management of employees and customer relations."

Further, the Staff's precedent regarding procedures for protecting customer information, including information transmitted via the Internet or stored electronically, is consistent with earlier Staff decisions finding that a wide variety of activities related to a company's management of customer relations is part of a company's ordinary business operations; therefore, shareholder proposals related to such matters are excludable under Rule 14a-8(i)(7). For example, in *Zions Bancorporation* (avail. Feb. 11, 2008, *recon. denied* Feb. 29, 2008), the Staff concurred with the exclusion of a proposal that requested that the board implement a mandatory adjudication process prior to termination of certain customer accounts, finding that the proposal related to "ordinary business operations (i.e., procedures for handling customers accounts)." Similarly, in *General Motors Corp.* (avail. Feb. 13, 1979), the Staff concurred with the exclusion of a shareholder proposal recommending the creation of a new department to handle customer complaints. In addition, in *OfficeMax Inc.* (avail. Feb. 13, 2006), the Staff permitted exclusion of a proposal directing the company to establish a task force regarding the handling of promotional rebates as relating to customer relations. *See also Wal-Mart Stores, Inc.* (avail. Mar. 27, 2001) (proposal seeking the implementation of annual customer meetings was excludable as ordinary business).

Similar to the above precedent that relates to the privacy and protection of customer information specifically and relationships with customers generally, the Proposal is excludable because it relates to the protection of the Company's customers' information and privacy. By requesting a report "explaining how the Board is overseeing privacy and data security risks," the Proposal addresses a central aspect of the Company's business. Due to the nature of its business, the Company's operations inherently involve collecting Internet payments and customer account data related to payment and delivery of products sold on the Company's websites. The Company serves consumers through its retail websites, and the online nature of the Company's business requires it to collect personal information from consumers, including consumers' names, addresses, e-mail addresses, Amazon.com account passwords and credit and debit card numbers. The Company also offers cloud-storage solutions, which allow the Company to store substantial amounts of data uploaded by third-party corporate customers, to enterprises through its Amazon Web Services business. In addition, the Company's network stores its own confidential data and information from sellers, suppliers, and content creators.

Thus, a significant portion of the Company's business is dependent on protecting the data and privacy of its customers and other third parties and ensuring that all data that the Company stores is secure. The Company uses multiple methods and processes to protect privacy and secure data, and the Board's and management's oversight of these data security methods and processes is a central aspect of the day-to-day management and oversight of the Company's business, as a material breach in the Company's data security systems could adversely affect the Company's operating results, result in litigation or potential liability and otherwise harm the Company's business. This oversight requires frequent interaction with skilled Company employees with specialized and in-depth knowledge regarding the Company's privacy controls and data security systems. Given the importance of data security to the Company's business and the specialized nature of privacy and data security, oversight of these issues are "so fundamental" to the Board's and management's ability to run the Company that they could not, as a practical matter, be subject to shareholder oversight. Therefore, the proposal is excludable under Rule 14a-8(i)(7).

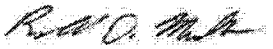
Finally, the Proposal does not raise a significant policy issue. As described above, the Staff has consistently concurred that proposals requesting reports on the protection of customer privacy, including customer data with respect to Internet privacy, are excludable as relating to ordinary business. Data security and customer privacy, while vital for the Company and an important function of management and the Board, are not significant policy issues. Rather, Internet privacy and data security are technical issues, the oversight of which require Board and management interaction with employees with specialized knowledge, and may not be easily understood, much less managed, by shareholders. In this regard, the Proposal does not focus on a significant policy issue, but rather relates to the technical issues on how the Company is overseeing and managing the protection of confidential data. *Cf., e.g., Verizon Communications Inc.* (avail. Feb. 13, 2012) (Staff did not concur in exclusion of net neutrality proposal and found net neutrality to be a significant policy issue "[i]n view of the sustained public debate over the last several years concerning net neutrality."). In contrast to net neutrality, the Board's oversight of privacy and data security is not a subject of sustained public debate, but rather relates to the Company's decisions on how to manage the day-to-day mechanics of the systems it has in place to protect the confidential information of the Company, its customers, and other parties. In this respect, it is important to note that in the Division of Corporation Finance's Disclosure Guidance: Topic No. 2 (Cybersecurity) (Oct. 13, 2011), the Division stated, "We prepared this guidance to be consistent with the relevant disclosure considerations that arise in connection with any business risk." Thus, as with the proposal discussed above in *The Western Union Co.*, the Proposal "requests a report that describes how [the Company] monitors and controls" just some of the many "particular risks" that the Company faces in its day to day operations, and therefore likewise is excludable under Rule 14a-8(i)(7).

**CONCLUSION**

Based upon the foregoing analysis, we respectfully request that the Staff concur that it will take no action if the Company excludes the Proposal from its 2013 Proxy Materials.

We would be happy to provide you with any additional information and answer any questions that you may have regarding this subject. Correspondence regarding this letter should be sent to shareholderproposals@gibsondunn.com. If we can be of any further assistance in this matter, please do not hesitate to call me at (202) 955-8671 or Sarah Dods, the Company's Senior Corporate Counsel, at (206) 266-3192.

Sincerely,



Ronald O. Mueller

Enclosures

cc: Sarah Dods, Amazon.com, Inc.
Joseph F. Keefe, Pax World Mutual Funds
Corey Johnson, Pax World Mutual Funds

101435470_8.DOCX

**EXHIBIT A**

PAX



December 7, 2012

David A. Zapolsky
Vice President, General Counsel and Secretary
Amazon.com, Inc.
410 Terry Avenue North
Seattle, WA 98109

Dear Mr. Zapolsky:

On behalf of Pax World Mutual Funds ("Pax World"), I write to give notice that, pursuant to the 2012 proxy statement of Amazon.com, Inc. (the "Company"), Pax World intends to present the attached proposal (the "Proposal"), regarding Privacy and Data Security, at the 2013 Annual Meeting of shareholders (the "Annual Meeting"). Pax World requests that the Company include the Proposal in the Company's proxy statement for the Annual Meeting. Pax World has owned the requisite number of the Company's shares for at least one year, continuously, and intends to hold these shares through the date on which the Annual Meeting is held.

I represent that Pax World or its agent intends to appear in person or by proxy at the Annual Meeting to present the attached Proposal. We have attached a letter confirming our proof of ownership. Please contact Corey Johnson by email at cjohnson@paxworld.com or by phone at (603) 501-7355 if you have any questions regarding this matter.

Sincerely,

Joseph F. Keefe
*President & CEO*
Pax World Mutual Funds

Encl. Resolution Text
Proof of Ownership Letter

## Privacy and Data Security

Whereas,

As a leader in online retailing, entertainment media, and cloud computing services to businesses, Amazon.com ("Amazon") confronts serious privacy and data security risks.

Breaches of privacy and data security are a growing threat which can result from company negligence or external attacks. Cyberattacks on U.S. computer networks rose 17-fold from 2009 to 2011, according to the National Security Agency.[i]

According to a 2011 Ponemon Institute study, the per capita cost of a data breach was $194, with an average incident cost of $5.5 million.[ii] A separate Ponemon study found data breaches could negatively impact brand value and reputation by as much as 12 percent to 25 percent, with the average loss in brand value ranging from $184 million to more than $330 million.[iii]

Unauthorized collection, disclosure, or misuse of personal information can cause great harm to individuals and society - including discrimination, identity theft, financial loss, loss of business or employment opportunities, humiliation, reputational damage, questionable government surveillance, or physical harm.

The Electronic Frontier Foundation said in a 2012 report[iv]: "Amazon is entrusted with huge quantities of information as part of its cloud computing services and retail operations, yet does not produce annual transparency reports, publish a law enforcement guide, or promise to inform users when their data is sought by the government."

In 2012 Amazon's Zappos unit and an affiliated site were the victims of a data breach which exposed personal information of more than 24 million customers, resulting in a consolidated class action lawsuit.[v] The New York Times observed: "The breaches at Amazon's sites, combined with several recent cyberattacks, could threaten to shake consumer confidence online."[vi]

We believe Amazon's Board has a fiduciary and social responsibility to protect company assets, including the personal information of a variety of stakeholders.

**Resolved,** that the Board of Directors publish a report, at reasonable expense and excluding confidential or proprietary information, explaining how the Board is overseeing privacy and data security risks.

**Supporting Statement**

We emphasize that the Proposal is not asking the Company to disclose risks, specific incidents, or legal compliance procedures; rather, we believe, investors need to understand more fully how the Board oversees the concerns described above.

Carnegie Mellon University's Cylab published a 2012 report ("How Boards and Senior Executives Are Managing Cyber Risks"[vii]) which we believe could be instructional in writing this report. Among Cylab's recommendations for boards:

"Review existing top-level policies to create a culture of security and respect for privacy. Organizations can enhance their reputation by valuing cyber security and the protection of privacy and viewing it as a corporate social responsibility."

"Review assessments of the organization's security program and ensure that it comports with best practices and standards and includes incident response, breach notification, disaster recovery, and crisis communications plans."

"Conduct an annual review of the enterprise security program and effectiveness of controls, to be reviewed by the board Risk Committee, and ensure that identified gaps or weaknesses are addressed."

---

[i] http://www.bloomberg.com/news/2012-08-29/sec-guidance-on-cyber-disclosure-becomes-rule-for-google.html

[ii] http://www.cbiz.com/ras/pdfs/2011_Ponemon_Study.pdf

[iii] http://www.worldnews.se/news/60845/new-survey-by-the-ponemon-institute-finds-that-data-breaches-can-cause-lasting-a/

[iv] https://www.eff.org/pages/who-has-your-back

[v] http://www.topclassactions.com/lawsuit-settlements/lawsuit-news/1575-zappos-hack-leads-to-class-action-lawsuit

[vi] http://bits.blogs.nytimes.com/2012/01/17/even-big-companies-cannot-protect-their-data/

[vii] http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf


December 7, 2012

Corey Johnson
Sustainability Research Analyst
Pax World Management LLC
30 Penhallow Street, Suite 400
Portsmouth, NH 03801

RE: Amazon.com, Inc. (023135106)

Dear Mr. Johnson,

State Street Bank & Trust Co., DTC Participant Code 0997, acts as custodian for the assets of the Pax World portfolio(s) listed below. This letter confirms that the Pax World Fund(s) listed below has/have continuously held shares of Amazon.com, Inc. with Cusip 023135106 with a market value of at least $2,000 for a period of one year as of December 7, 2012.

Amazon.com, Inc.
023135106

PAX WORLD GROWTH FUND
5000.000 Shares Held as of December 7, 2012
State Street *** FISMA & OMB Memorandum M-07-16 ***

Sincerely,

Mark J Howcroft
Officer

GIBSON DUNN

Gibson, Dunn & Crutcher LLP

1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306
Tel 202.955.8500
www.gibsondunn.com

Ronald O. Mueller
Direct: +1 202.955.8671
Fax: +1 202.530.9569

Client: 03981-00145

December 21, 2012

VIA OVERNIGHT MAIL

Joseph F. Keefe
President & CEO
Pax World Mutual Funds
30 Penhallow Street, Suite 400
Portsmouth, NH 03801

Dear Mr. Keefe:

I am writing on behalf of our client, Amazon.com, Inc. (the "Company"), which received on December 10, 2012, the shareholder proposal you submitted on behalf of Pax World Mutual Funds ("Pax World") entitled "Privacy and Data Security" for consideration at the Company's 2013 Annual Meeting of Shareholders (the "Proposal").

The purpose of this letter is to inform you that the Proposal contains certain procedural deficiencies, which Securities and Exchange Commission ("SEC") regulations require us to bring to your attention. Rule 14a-8(d) of the Exchange Act requires that any shareholder proposal, including any accompanying supporting statement, not exceed 500 words. The Proposal, including the supporting statement, exceeds 500 words. In reaching this conclusion, we have counted dollar symbols as words and have counted each number associated with a footnote every time that number appears. To remedy this defect, Pax World must revise its Proposal such that it does not exceed 500 words and submit the revised Proposal to the Company.

The SEC's rules require that any response to this letter be postmarked or transmitted electronically no later than 14 calendar days from the date you receive this letter. Please address any response to me at Gibson, Dunn & Crutcher LLP, 1050 Connecticut Ave., N.W., Washington, D.C. 20036. Alternatively, you may transmit any response by facsimile to me at (202) 530-9569.

If you have any questions with respect to the foregoing, please contact me at (202) 955-8671. For your reference, I enclose a copy of Rule 14a-8.

Sincerely,

Ronald O. Mueller

Enclosures

cc: Sarah C. Dods, Senior Corporate Counsel, Amazon.com, Inc.
Corey Johnson, Pax World Mutual Funds

101431174.2

PAX

December 28, 2012

Ronald O. Mueller
Gibson, Dunn & Crutcher LLP
1050 Connecticut Avenue, N.W.
Washington, DC 20036-5306

Dear Mr. Mueller:

On December 26, 2012, Pax World Mutual Funds ("Pax World") received your letter regarding certain procedural deficiencies identified in its shareholder proposal (the "Proposal") to Amazon.com. Pursuant to Rule 14a-8(d) of the Exchange Act, Pax World has revised the Proposal to include no greater than 500 words.

Sincerely,

Corey Johnson
*Sustainability Research Analyst*
Pax World Mutual Funds

Encl. Revised Shareholder Resolution

**Privacy and Data Security**

Whereas,

As a leader in online retailing, entertainment media, and cloud computing services, Amazon.com ("Amazon") confronts serious privacy and data security risks.

Privacy and data security breaches are growing threats that can result from company negligence or external attacks. The National Security Agency reported that cyberattacks on U.S. computer networks rose 17-fold from 2009 to 2011.[i]

According to a 2011 Ponemon Institute study, the per capita cost of a data breach was $194, with an average incident cost of $5.5 million.[ii] Another Ponemon study found data breaches could negatively impact brand value and reputation by as much as 12 percent to 25 percent, with average losses in brand value ranging from $184 million to more than $330 million.[iii]

Unauthorized collection, disclosure, or misuse of personal information can cause significant harm to individuals and society - including discrimination, identity theft, financial loss, reputational damage, questionable government surveillance, or physical harm.

The Electronic Frontier Foundation said in a 2012 report[iv]: "Amazon is entrusted with huge quantities of information as part of its cloud computing services and retail operations, yet does not produce annual transparency reports, publish a law enforcement guide, or promise to inform users when their data is sought by the government."

In 2012 Amazon's Zappos unit was the victim of a data breach that exposed personal information of more than 24 million customers, resulting in a consolidated class action lawsuit.[v] The New York Times observed: "The breaches at Amazon's sites, combined with several recent cyberattacks, could threaten to shake consumer confidence online."[vi]

We believe Amazon's Board has a fiduciary and social responsibility to protect company assets, including the personal information of its stakeholders.

**Resolved,** that the Board of Directors publish a report, at reasonable expense and excluding confidential or proprietary information, explaining how the Board is overseeing privacy and data security risks.

**Supporting Statement**

We emphasize that the Proposal is not asking the Company to disclose risks, specific incidents, or legal compliance procedures; rather, we believe, investors need to better understand how the Board oversees the concerns described above.

Carnegie Mellon University's Cylab published a 2012 report ("How Boards and Senior Executives Are Managing Cyber Risks"[vii]) that we believe could be instructional in writing this report. Among Cylab's recommendations for boards:

"Review existing top-level policies to create a culture of security and respect for privacy. Organizations can enhance their reputation by valuing cyber security and the protection of privacy and viewing it as a corporate social responsibility."

"Review assessments of the organization's security program and ensure that it comports with best practices and standards and includes incident response, breach notification, disaster recovery, and crisis communications plans."

"Conduct an annual review of the enterprise security program and effectiveness of controls, to be reviewed by the board Risk Committee, and ensure that identified gaps or weaknesses are addressed."

---

[i] http://www.bloomberg.com/news/2012-08-29/sec-guidance-on-cyber-disclosure-becomes-rule-for-google.html

[ii] http://www.cbiz.com/ras/pdfs/2011_Ponemon_Study.pdf

[iii] http://www.worldnews.se/news/60845/new-survey-by-the-ponemon-institute-finds-that-data-breaches-can-cause-lasting-a/

[iv] https://www.eff.org/pages/who-has-your-back

[v] http://www.topclassactions.com/lawsuit-settlements/lawsuit-news/1575-zappos-hack-leads-to-class-action-lawsuit

[vi] http://bits.blogs.nytimes.com/2012/01/17/even-big-companies-cannot-protect-their-data/

[vii] http://www.rsa.com/innovation/docs/CMU-GOVERNANCE-RPT-2012-FINAL.pdf