EBAY INC
Form PX14A6G
April 17, 2013

Trillium Asset Management, LLC
711 Atlantic Avenue
Boston, MA 02111

April 8, 2013

Dear eBay Inc. Shareholders,

We are writing to urge you to VOTE "FOR" PROPOSAL 4 on the proxy card, which asks the Company how it is managing the privacy and data security risks associated with the Company's operations and new PayPal venture.1

The shareholder proposal makes the following request of eBay:

The Company's 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."

Privacy and data security have quickly become one of the most critical business and social issues of our time. They are especially important for companies like eBay whose business depends on large amounts of personal information about their customers.

PayPal is the fastest-growing segment of eBay's business, a global online payment company with 123 million active registered accounts available in 190 markets around the world. PayPal revenues for Q4 2012 were $1.54 billion, growing 24 percent year over year and representing 39 percent of eBay Inc. revenues in that period.2

PayPal is poised to introduce a major new payment service in retail outlets in the U.S. and around the world. This initiative, years in the planning, offers the company opportunity – and significant risks.

According to published reports, the new PayPal retail payment service will rely heavily on large amounts of personal consumer information that will allow retailers to offer highly-customized marketing and advertising messages. This type of advertising has increasingly been the subject of intense scrutiny by federal and state regulators and legislators.

We are concerned that issues of privacy and data security increasingly present eBay with significant regulatory, legal, financial and reputational risks. While we are pleased that the Company has amended the Audit Committee's charter to include privacy and security matters following our suggestion and dialog, we believe shareholders would be well served by a report explaining how the Board is overseeing privacy and data security risks.

PayPal Payment Service

PayPal has announced plans to enter the retail payment business in 2013 with a service that combines the use of online and offline data. According to published reports, the service will allow shoppers to use "their mobile phones, PIN or a plastic card made to look like a credit card to pay at the cash register, potentially heralding the biggest transformation of the company's business model yet."3

1 IMPORTANT NOTICE: The cost of this communication is being borne entirely by Trillium Asset Management, LLC. Trillium is NOT asking for your proxy card and is not providing investment advice. We will not accept proxy cards, and any proxy cards received will be returned.

2 https://www.paypal-media.com/mediacenter.cfm

3 http://www.cfo-insight.com/human-capital-career/interviews/paypal-cfo-patrick-dupuis-on-transformational-change/

According to the Company and published reports, the payment service will be available at more than 7 million retail locations through the Discover card network,4 at 23 major national retailers5 (including Home Depot, Office Depot, and Toys “R” Us), as well as gas station and convenience store chains,6 and restaurants and retailers using NCR technology.7

The PayPal retail payment service represents a major change in eBay’s business model. According to a report in CFO Insight, quoting eBay Chief Financial Officer Patrick DuPuis:

While PayPal, not being publicly listed, will not reveal anything about the revenues expectations it is pinning to the new service, the foray into offline has already begun to redefine the way the company presents itself to the outside world. "In the fourth quarter of last quarter we took the 'e' out of the definition of our mission. It's now 'connected commerce', not e-commerce," CFO Patrick Dupuis tells CFO Insight in an interview. Eventually, he hopes, PayPal will become the "wallet" for consumers, who will use it to store their credit card data and account information.8

A major concern is the Company’s intention to use offline and online data to offer a form of targeted advertising that many consumers could see as an invasion of their privacy. In a media interview, PayPal vice president Don Kingsborough, who has helped lead development of the new service, said it would likely employ forms of highly targeted advertising and marketing:

But the other important winning determinant will be providing valuable, relevant and easy-to-use services to consumers, becoming the one mobile wallet they turn to, said Kingsborough. He said using tools like WHERE’s targeting and location technology will allow merchants to not just push out deals but deliver very context-aware content. For example, he said a clothes retailers might be able to message a nearby customer, letting them know they’ll earn $5 in their PayPal account that day if they buy jeans that they’ve purchased in the past. And, with the right permissions, the merchant may also be able to know the customer is with two friends and offer a group discount.9

One writer, following an interview with PayPal president David Marcus, expressed it this way:

You may wonder how exactly I could categorize this as a risk, particularly given that the company isn't really stepping out into a world that hasn't already shown proven growth potential. The reality, however, is that many who aren't tightly connected to internet commerce have never even heard of PayPal. And for many who have, they certainly haven't gone out of their way to use it. Next year, that all changes. Suddenly, PayPal will be labeling itself on the doors of businesses large and small, right alongside the iconic Visa and MasterCard icons that are now synonymous with "trusted payment processors." Suddenly, PayPal will thrust itself into the mainstream. Suddenly, any privacy violation or database hack won't just make the rounds on your favorite technology sites, it'll hit the teleprompters in front of Brian Williams and Will McAvoy.10

4http://online.wsj.com/article/SB10000872396390444358404577605072602107932.html
5https://www.paypal-promo.com/anywhere/desktop/#retailers
6https://www.thepaypalblog.com/2013/02/paypal-coming-to-neighborhood-gas-station-near-you-2/
7http://www.marketwatch.com/story/ncr-and-paypal-working-together-to-make-everyday-easier-for-consumers-when-dining-o
8http://www.cfo-insight.com/human-capital-career/interviews/paypal-cfo-patrick-dupuis-on-transformational-change/
9 http://gigaom.com/2012/01/14/paypals-don-kingsborough-in-store-payment-is-ours-to-lose/
10 http://www.engadget.com/2012/12/10/paypal-interview-david-marcus-customer-service/

Privacy and Data Security Risks

The combination of offline and online data, and mobile payment systems, represents new technology and new forms of interaction with consumers, potentially presenting an emerging threat to privacy and data security.

Regulatory Risk:

Data collection practices are increasingly drawing the attention of regulators. We believe these concerns apply to many of the practices that appear to be employed in the new PayPal payment service.

In December 2012, the Federal Trade Commission (FTC) announced that it had opened an inquiry into the practices of nine data brokers that collect and resell or analyze consumer data. “Data brokers aggregate huge amounts of data on individuals and have the capacity to create powerful profiles combining information about what you do offline and online,” said David C. Vladeck, director of the Bureau of Consumer Protection at the FTC . “We worry that this information may be used in ways that could be harmful to consumers.”11

In addition to data collection practices, the proposal addresses concerns related to data security. Indeed, President Obama has 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.”12 Senator John D. Rockefeller IV (D., W.Va.) recently sent a letter to the CEOs of all Fortune 500 companies asking the companies for more information about their cyber security practices. 13

Brand & Litigation Risk:

As noted in the Proposal and Company Opposition statement, eBay has been recognized by the Ponemon Institute as one of the “Most Trusted Companies for Privacy.” For this exact reason, we believe a shift in perception could limit future growth. We would also note that eBay has fallen in the top ten ranking from #1 in 2006 to #9 in 2012.14 A further drop in ranking may indicate a negative trend for eBay’s brand value.

In research that has been submitted to the FTC, analysts at the Berkeley Center for Law and Technology, conclude that “Americans overwhelmingly reject mobile payment systems that track their movements or share identification information with retailers.”

Based on surveys conducted in January 2012, the researchers said:15

We found that Americans overwhelmingly oppose the revelation of contact information (phone number, email address, and home address) to merchants when making purchases with mobile payment systems. Furthermore, an even higher level of opposition exists to systems that track consumers’ movements through their mobile phones.

We asked Americans whether they thought that phones should share information with stores when they visit and browse without making a purchase. Overwhelmingly, subjects rejected this possibility. Ninety-six percent objected to such tracking, with 79 percent stating that they would “definitely not allow” it and 17 percent stating that they would “probably not allow” it.

---

11 http://ftc.gov/opa/2012/12/databrokers.shtm
12http://www.whitehouse.gov/cybersecurity
13http://commerce.senate.gov/public/?a=Files.Serve&File_id=396eb5d5-23a4-4488-a67c-d45f62bbf9e5

14 http://www.ponemon.org/local/upload/file/2012%20MTC%20Report%20FINAL.pdf
15 http://www.ftc.gov/os/comments/mobilepayments/561018-00021-82938.pdf

The study notes that PayPal's mobile payment system is among those that "appear" to "collect Level 3 data about consumers' purchases," a major change from traditional credit card practices. These new data collection techniques represent a dramatic change in considerations of consumer privacy.

With these capabilities, all of the service providers in the payments ecosystem—merchants, payment networks, and the banks involved in the transactions—could develop much more comprehensive and detailed dossiers about consumer purchase behavior than they typically have today. The capabilities of new payment systems will, for example, make it easier for merchants to build customer databases without resorting to loyalty cards.

This possible shift has profound consequences for consumer privacy and the relationship consumers have with payment providers and merchants. The need for loyalty cards will be eliminated, but so too could the ability of individuals to avoid profiling. Many consumers have long been uncomfortable with information collection surrounding their purchases. Such information collection could cause embarrassment, lead consumers to avoid buying certain items, or possibly contribute to systems that institute widespread service and price discrimination.

As the Proposal notes, 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. Additionally, customer aversion to privacy risk could limit eBay's PayPal service adoption and ultimate revenue opportunity.

Importantly, we note that in addition to privacy, the Proposal also addresses concerns related to data security – a topic that has been featured widely in media accounts with reports of hacking at media enterprises such as The New York Times and The Wall Street Journal, and even sophisticated tech ventures such as Twitter. Breaches of privacy and data security are a growing threat which can result from company negligence or external attacks. One study by the Ponemon Institute entitled, "Reputation Impact of a Data Breach," has found data breaches could negatively impact brand value and reputation by as much as 17 percent to 31 percent, with the average loss in brand value ranging from $184 million to more than $330 million.16

The Role of the Board of Directors

The Board's Statement of Opposition to the shareholder proposal fails to address the risks associated with the Company's new priorities and the introduction of the new PayPal mobile payment processing system.

While we appreciate the Company's amendment of the Audit Committee's charter to include privacy and security language following our suggestion and dialog, the Company's Opposition Statement does not provide any insight into our core concern: explaining how the Board is overseeing privacy and data security risks.

A recitation of policies and practices by management is certainly welcome. But it does not explain, for example, how these policies and practices address the risks presented by an entirely new service which, according to experts, could involve privacy breaches, controversies related to consumer profiling, litigation, and a loss in eBay's brand value. Further, existing policies do not provide any insight into the Board's oversight and appraisal of these risks because they are not from the Board of Directors.

A recent survey by Carnegie Mellon University's Cylab of Forbes 2000 Global companies found that:

"…boards are not actively addressing cyber risk management. While placing high importance on risk management generally, there is still a gap in understanding the linkage between information technology (IT) risks and enterprise risk management. Although there have been some measureable improvements since the 2008 and 2010 surveys,

boards still are not undertaking key oversight activities related to cyber risks, such as reviewing budgets, security program assessments, and top-level policies; assigning roles and responsibilities for privacy and security; and receiving regular reports on breaches and IT risks. Involvement in these areas would help them manage reputational and financial risks associated with the theft of confidential and proprietary data and security breaches of personal information."

16 http://media.scmagazineus.com/documents/30/ponemon_reputation_impact_of_a_7405.pdf

We believe a report adequate for an investor to assess privacy and data security risk could draw from the 2012 Carnegie Mellon University's Cylab report ("How Boards and Senior Executives Are Managing Cyber Risks"), which recommends 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."

- "Require regular reports from senior management on privacy and security risks."

Additionally, we believe shareholders would best be served by additional transparency into how the Board is overseeing privacy risk as it relates to the PayPal retail venture, as this opportunity exposes the Company directly to the risks outlined in this memo, and could limit shareholder value creation.

Conclusion

Given how important brand value is to the company's growth and the risks that data privacy and security present, we believe the company's current level of disclosure is woefully inadequate.

We strongly believe the Board of Directors needs to report to shareholders describing how the Board is overseeing and will oversee privacy and security risks, particularly as it relates to the new PayPal venture.

For all of the reasons provided above, we strongly urge you to VOTE FOR PROPOSAL 4. Considering how important privacy and data security is to eBay's financial prosperity, the risks posed to the business by combining online and offline customer data as well as mobile payment technology are concerning and the Company's failure to provide a meaningful assessment of this material issue is dramatic.

Please contact Natasha Lamb at nlamb@trilliuminvest.com or 978-578-4123 for additional information.

Sincerely,

Natasha Lamb
Vice President
Shareholder Advocacy & Corporate Engagement
Trillium Asset Management, LLC