AMERICAN EXPRESS CO
Form PX14A6G
April 25, 2014
April 23, 2014

Natasha Lamb
Arjuna Capital/Baldwin Brothers Inc.
204 Spring Street
Marion, MA 02738
978-578-4123, natasha@arjuna-capital.com

Dear American Express Shareholders,

We are writing to urge you to VOTE “FOR” PROPOSAL 5 on the proxy card, which asks the Company to publish a report on privacy and data security risks, with specific emphasis on government requests for customer information.1

The shareholder proposal makes the following request of American Express:

Shareholders request that the Company publish an annual report explaining how the Board is overseeing privacy and data security risks, providing metrics and discussion, subject to existing laws and regulation, regarding requests for customer information by U.S. and foreign governments, at reasonable cost and omitting proprietary information.

After reviewing the proposal, Institutional Shareholder Services (a division of MSCI and the leading provider of proxy voting advice) has recommended a vote in favor of the proposal:

A vote FOR this proposal is warranted as additional disclosure of the company's board oversight of privacy and data security risks would aid shareholders in understanding how the company is managing potential risks associated with data security.

The business, brand, and regulatory risks highlighted below are formally acknowledged by the Company and are of critical concern to shareholders. Given the evolving risk landscape, we believe implementing the steps suggested in the Proposal would provide needed transparency and confidence that management and the board are properly managing and overseeing these risks. There is a great deal of movement by corporations to provide privacy and data security disclosures incited by pressure from the public at large, government, and non-governmental organizations. American Express shareholders should be provided the transparency necessary to understand the Company’s exposure to and management of these risks.

We believe shareholder should vote “FOR” the proposal for the following reasons:

- Privacy and Data Security are Critical Concerns:
  - Major “hacks” of confidential customer data (often involving credit card data) and disclosures of extensive government surveillance (reportedly involving requests of data from credit card companies) have heightened public concern over these issues and increased potential legal, financial and reputational risk for the Company.
  - 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.
- American Express Lags Peers in Disclosure of Government Requests for Customer Information:

1 IMPORTANT NOTICE: The cost of this communication is being borne entirely by Arjuna Capital. Arjuna 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.

- MasterCard has responded proactively to shareholder concerns by issuing a "Privacy & Data Protection" report addressing government surveillance, privacy, and data security.2
- Privacy, data security, and government surveillance risk cut across sectors and industries. Most leading consumer-facing Internet companies (including Google, Facebook, Microsoft, Yahoo!, Twitter and LinkedIn) as well as the leading U.S. telecommunications carriers (AT&T and Verizon) now regularly publish "transparency reports" detailing government and law enforcement requests for confidential customer data.
- In order for shareholders to have the necessary understanding of how American Express is responding to these issues, we believe the Company should issue a report providing much greater detail, as put forth in the Proposal.

• Mismanagement of Privacy and Data Security Carries Risks for American Express:

- As one of the world's leading financial services companies, American Express has a duty to protect both customer privacy and the security of customer data.
- A failure to do so carries significant business risks including: potentially significant regulatory and/or governmental investigations and/or actions, litigation, fines, sanctions and damage to our global reputation and our brand.3

Privacy and Data Security Are Critical Concerns

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.

Major "hacks" of confidential customer data (often involving credit card data) and disclosures of extensive government surveillance (reportedly involving requests of data from credit card companies) have heightened public concern over these issues and increased potential legal, financial and reputational risk for the Company.

Government Surveillance
The disclosures in 2013 of extensive surveillance programs by the U.S. National Security Agency and other government agencies have triggered unprecedented attention to the issues of privacy and data security. By one estimate, disclosures of spying abroad may cost U.S. companies as much as $35 billion in lost revenue through 2016 because of doubts about the security of information on their systems.4

These disclosures have important implications for American Express and the financial services industry in the form of legal, financial, and reputational risk.

There is controversy associated with American Express and credit card companies surrounding consumer privacy and data security:

In June 2013, The Wall Street Journal reported that the "National Security Agency's monitoring of Americans includes customer records from the three major phone networks as well as emails and Web searches, and the agency also has cataloged credit-card transactions, said people familiar with the agency's activities."5 [Proponent's emphasis]

TIME reported that credit card networks "are most likely giving the government 'metadata.' That is, the credit card issuers could provide the NSA details such as an account or card number, where and when a purchase was made, and for how much."6 [Proponent's emphasis]

2 http://investorrelations.mastercardintl.com/phoenix.zhtml?c=148835&p=irol-Protection
3 https://www.sec.gov/Archives/edgar/data/4962/000119312514066777/d656045d10k.htm

4 http://www.bloomberg.com/news/2013-11-26/nsa-spying-risks-35-billion-in-u-s-technology-sales.html
5 http://online.wsj.com/news/articles/SB10001424127887324299104578529112289298922?mg=reno64-wsj
6 http://business.time.com/2013/06/11/big-brother-is-watching-you-swipe-the-nsas-credit-card-data-grab/

SPIEGEL magazine, relying on documents provided by Edward Snowden, reported that there is within the NSA an ongoing data-gathering initiative known as "Follow the Money" which spies on payments processed by major credit card processing networks. In 2011, that database reportedly held 180 million records, with 84 percent of them credit card transactions.7 [Proponent's emphasis]

In response to a request for comment, an NSA spokesperson sent the following statement to at least one media outlet:

The U.S. Government acquires information about economic and financial matters to combat a range of threats to the national security of the United States and its allies, including information about terrorist financing and terror networks. This information is collected through regulatory, law enforcement, diplomatic, and intelligence channels, as well as through undertakings with cooperating foreign allies and partners.8

The degree to which companies cooperate with government and law enforcement requests for confidential customer information has become a critical concern for shareholders.

American Express Lags Peers in Disclosure of Government Requests for Consumer Information

Privacy, data security, and government surveillance risk cut across sectors. Most leading consumer-facing Internet companies (including Google, Facebook, Microsoft, Yahoo!, Twitter and LinkedIn) as well as the leading U.S. telecommunications carriers (AT&T and Verizon) now regularly publish "transparency reports" detailing government and law enforcement requests for confidential customer data. MasterCard has responded to shareholder concerns by issuing a "Privacy & Data Protection" report.9

Indeed, within the last six months, shareholder proposals at Verizon Communications Inc. and AT&T Inc. have requested that the companies issue regular reports regarding requests for customer data. In December 2013, both Verizon and AT&T agreed to publish reports and did so early in 2014.10 11 As a result, shareholder proposals at both companies were withdrawn.12 13

Verizon, in publishing its first transparency report, said14:

"The past year saw an intense focus around the world on government demands to obtain customer data…we believe this Transparency Report will add to the ongoing conversation about privacy and public safety."

Under the headline, "Our commitment to you," AT&T commented15:

"Interest in this topic has increased in the last year. As you might expect, we may make adjustments to our reporting processes and create ways to track forms of demands in the future. We're committed to providing you with as much transparency and accuracy in this reporting as is possible. This includes:

7 http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html
8 http://news.cnet.com/8301-1009_3-57603076-83/nsa-snoops-on-credit-card-transactions-says-report/
9 http://investorrelations.mastercardintl.com/phoenix.zhtml?c=148835&p=irol-Protection
10 http://transparency.verizon.com/us-data
11 http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html
12 http://online.wsj.com/article/BT-CO-20140219-708411.html
13
http://www.trilliuminvest.com/news-articles-category/thinking-capital/investors-withdraw-verizon-shareholder-proposal-on-go

14 http://publicpolicy.verizon.com/blog/entry/verizon-releases-first-transparency-report
15 http://about.att.com/content/csr/home/frequently-requested-info/governance/transparencyreport.html

- Including new information as we are allowed by government policy changes.
- Considering ways to enhance the detail provided in this report as we begin to track these demands consistent with what can be reported publicly."

Reports detailing government and law enforcement requests for confidential customer data are now also routinely published by Google16, Microsoft17, Facebook18, Yahoo!19, LinkedIn20, Apple21, Twitter22 and other consumer-facing Internet companies.

Importantly, MasterCard has proactively responded to shareholder concerns by issuing a "Privacy & Data Protection" report.23 The report addresses "Government Requests for Data" among other concerns noted in this memo. While we view this disclosure as a first step, it is a strong example of how an industry peer is addressing the issue head on.

While privacy is critical to the success of American Express's business, the Company has not disclosed information regarding the extent and nature of requests for customer data made by government agencies. We believe American Express has an obligation to its customers and shareholders to abide by what is fast emerging as best practice for consumer-facing companies that control large amounts of confidential customer information.

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, investigation by numerous non-governmental organizations, and an extraordinary amount of media attention.

Data Security
Protecting consumer privacy through data security has become a nation-wide and international priority, which has only been strengthened by controversy over government requests for consumer information and the rise of "big data." We believe American Express stands to be impacted by increased regulation dictating consumer data use and security.

In February 2012, the Obama Administration unveiled a "Consumer Privacy Bill of Rights"24 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 "seeks to protect all Americans from having their information misused by giving users new legal and technical tools to safeguard their privacy."

Based on globally accepted privacy principles originally developed in the United States, the Consumer Privacy Bill of Rights is a comprehensive statement of the rights consumers should expect and the obligations to which companies handling personal data should commit. These rights include the right to control how personal data is used, the right to avoid having information collected in one context and then used for an unrelated purpose, the right to have information held securely, and the right to know who is accountable for the use or misuse of an individual's personal data. [Proponent's emphasis]

16 https://www.google.com/transparencyreport/
17 http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
18 https://www.facebook.com/about/government_requests
19 http://info.yahoo.com/transparency-report/
20 http://blog.linkedin.com/2014/02/03/updated-linkedin-transparency-report-including-requests-related-to-u-s-national-security-r
21 http://images.apple.com/pr/pdf/140127upd_nat_sec_and_law_enf_orders.pdf
22 https://transparency.twitter.com/

23 http://investorrelations.mastercardintl.com/phoenix.zhtml?c=148835&p=irol-Protection

24 http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-priva

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.”26 [Proponent’s emphasis]

In January of this year, President Obama went further to appoint his counselor, John Pedesta, “to lead a comprehensive review of big data and privacy” that “will reach out to privacy experts, technologists and business leaders, and look how the challenges inherent in big data are being confronted by both the public and private sectors; whether we can forge international norms on how to manage this data; and how we can continue to promote the free flow of information in ways that are consistent with both privacy and security.“27

Target, one of America’s largest retail chains, recently disclosed breaches that are believed to have exposed personal data of as many as 110 million customers, more than a third of the population of the United States. At a hearing on the incident, Senator Patrick Leahy, chair of the Senate Judiciary Committee, said if consumers cannot trust businesses to keep their data secure, “our economic recovery is going to falter.”28 [Proponent’s emphasis]

The Securities and Exchange Commission Division of Corporation Finance recognized the importance and arrival of this issue in 2011 by issuing 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.29

Privacy and data security have attracted significant attention from leaders of the U.S. Congress. On January 2, 2014, House Majority Leader Eric Cantor, citied recent high profile data breaches at Target and other companies, expressed concerns over security of health care data, and noted that four separate House Committees (Science, Homeland Security, Energy & Commerce, and Oversight & Government Reform) have recently investigated the risks of data breaches in online exchanges.30

In January 2014, Sen. Patrick Leahy re-introduced a Senate bill to set one nationwide standard for data breach notification—presently, 46 states have their own data breach notification laws—and mandate that consumers be told when their personal information has been compromised.31

26 http://www.whitehouse.gov/cybersecurity
27 http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence
28 http://www.nytimes.com/2014/02/05/business/target-to-speed-adoption-of-european-anti-fraud-technology.html?hpw&rref=tec
29 CF Disclosure Guidance: Topic No. 2, Cybersecurity, October 13, 2011.
30 http://majorityleader.gov/blog/2014/01/memo-legislation-on-data-breaches-and-obamacare.html
31 http://blogs.wsj.com/riskandcompliance/2014/01/08/personal-data-privacy-bill-re-introduced-in-congress/

A front page New York Times story ("As Hacking Against U.S. Rises, Experts Try to Pin Down Motive"32) 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."

The foregoing highlights an evolving regulatory landscape that will dramatically shape how companies address current and emerging risks related to privacy and data security. As shareholders, we believe American Express needs to take a proactive stance in disclosing privacy risks to investors and stakeholders.

Mismanagement of Privacy and Data Security Carries Risks for American Express
As one of the world's leading financial services companies, American Express has a duty to protect both customer privacy and the security of customer data.

A failure to do so carries significant business risks including: potentially significant regulatory and/or governmental investigations and/or actions, litigation, fines, sanctions and damage to our global reputation and our brand.33

American Express recognizes the import and business implications of regulatory privacy risks in their 10-k: 34

Regulation in the areas of privacy, information security and data protection could increase our costs and affect or limit how we collect and/or use personal information and our business opportunities.

…legislators and/or regulators in the United States and other countries in which we operate are increasingly adopting or revising Privacy, Information Security and Data Protection Laws that potentially could have significant impact on our current and planned privacy, data protection and information security-related practices, our collection, use, sharing, retention and safeguarding of consumer and/or employee information, and some of our current or planned business activities. For example, the U.S. House of Representatives and Senate considered a number of privacy, security breach notification, cybersecurity and information-security related bills during the 113th Congress and various committee hearings were held on related subjects. There also continues to be legislative activity in these areas at the state level. New legislation or regulation could increase our costs of compliance and business operations and could reduce revenues from certain business initiatives. Moreover, the application of existing laws to technology developments can be uncertain, increasing compliance risk. [Proponent's emphasis]

Compliance with current or future Privacy, Data Protection and Information Security Laws to which we are subject affecting customer and/or employee data could result in higher compliance and technology costs and could restrict our ability to fully exploit our closed-loop capability or provide certain products and services, which could materially and adversely affect our profitability. Our failure to comply with Privacy, Data Protection and Information Security Laws could result in potentially significant regulatory and/or governmental investigations and/or actions, litigation, fines, sanctions and damage to our global reputation and our brand. In recent years, there has been increasing enforcement activity in the areas of privacy, data protection and information security in various countries in which we operate. [Proponent emphasis]

As a consumer facing company, American Express faces not only operational risks, but also risk to their brand and future revenue opportunities. A strong brand is reliant on consumer trust and we believe past trust can be eroded rapidly by failing to address current and emerging issues, such as government requests for information and the sale of "big data," head on. This perception may be compounded as peers such as MasterCard take a proactive approach to disclosure.

32 http://www.nytimes.com/2013/03/04/us/us-weighs-risks-and-motives-of-hacking-by-china-or-iran.html?hpw

33 https://www.sec.gov/Archives/edgar/data/4962/000119312514066777/d656045d10k.htm
34 https://www.sec.gov/Archives/edgar/data/4962/000119312514066777/d656045d10k.htm

There is controversy associated with American Express and credit card companies surrounding consumer privacy and data security: In April 2013, Advertising Age magazine reported35:

Credit-card firms are selling their credit-card transaction data for digital advertising and other marketing efforts, but they're not exactly broadcasting the fact for fear of consumer backlash.

Mastercard Advisors launched its Information Services division around two-and-a-half years ago and in recent months has been approaching media-agency trading desks with an enticing offer: data representing 80 billion consumer purchases.

American Express has also turned its transaction data into a revenue stream through its Business Insights consulting division which has aimed direct mail and online offers to card holders on behalf of advertisers for years, though on an aggregate level. More recently, AmEx has modeled audience segments for use in online ad targeting. The company declined to name any partners in the endeavor, but stressed the AmEx data models don't allow for direct targeting of its card holders.

This controversy was further reported by Consumer Affairs, quoting David Jacobs of the Consumer Protection Counsel at the Electronic Privacy Information Center (EPIC):

I think that individuals have a privacy interest in transparency and control regarding the use of their personal data for advertising. Unfortunately, there is currently a lack of transparency in the sale and aggregation of consumer information by data brokers and marketing companies.

These kinds of controversy may erode consumer trust and brand value. Jacobs went on to highlight the regulatory risk:

The legislation hasn’t been released yet, but the CPBR includes a comprehensive set of fair information practices such as control, transparency, and accountability that, if faithfully implemented, could improve consumer privacy and help address these practices. 36

The controversy above highlights the brand and regulatory risks associated with the potential mismanagement/abuse of consumer data. American Express also notes its data vulnerability to 3rd party relationships in the Company 10-k:

There is also a risk the confidentiality, privacy and/or security of data held by third parties or communicated over third-party networks or platforms could become compromised.37

Conclusion:
For all the reasons provided above, we strongly urge you to support the Proposal. Managing privacy and data security risk may have a direct impact on the profitability of American Express and we believe it is in the best interest of shareholders. Please contact Natasha Lamb at 978-578-4123 or natasha@arjuna-capital.com for additional information.

Sincerely,
Natasha Lamb, Director of Equity Research & Shareholder Engagement
Arjuna Capital/Baldwin Brothers, Inc.

35 http://adage.com/article/dataworks/mastercard-amex-feed-data-marketers/240800/

36
http://www.consumeraffairs.com/news/mastercard-amex-selling-customer-transaction-data-to-marketers-041913.html
37 https://www.sec.gov/Archives/edgar/data/4962/000119312514066777/d656045d10k.htm