AMERICAN EXPRESS CO
Form PX14A6G
May 07, 2015
May 5, 2015

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.

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.
- American Express Lags Peers in Disclosure of Government Requests for Customer Information:

- MasterCard has responded proactively to shareholder concerns by issuing a “Privacy & Data Protection” report addressing government surveillance, privacy, and data security.1
- Privacy, data security, and government surveillance risk cuts 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.
- The U.S Department of Justice has adopted a policy allowing companies to report on national security letters and requests from the Foreign Intelligence Surveillance Court. 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.

- 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, the focus of national and international lobbying campaigns, investigation by numerous non-governmental organizations, and an extraordinary amount of media attention.
- Regulatory risk has increased as a bi-partisan Data Security and Breach Notification Act was introduced to Congress in 2015

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.2

We believe best practice disclosure would include the following:

As noted in the supporting statement of the proposal:

In preparing these reports, the Company may omit information on routine requests under individualized warrants. The reports should consider existing Transparency (or Law Enforcement Request) Reports published by major Internet companies, and where applicable, include (1) how often AXP has shared information with U.S. or foreign government entities; (2) type of customer information shared; (3) number of customers affected; (4) type of government requests; and (5) discussion of Company efforts to protect customer privacy and data.

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.

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

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.3

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.”4 [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.”5 [Proponent’s emphasis]

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.6 [Proponent’s emphasis]

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

---

3 http://www.bloomberg.com/news/2013-11-26/nsa-spying-risks-35-billion-in-u-s-technology-sales.html
4 http://online.wsj.com/news/articles/SB10001424127887324299104578529112289298922?mg=reno64-wsj
5 http://business.time.com/2013/06/11/big-brother-is-watching-you-swipe-the-nsas-credit-card-data-grab/
6 http://www.spiegel.de/international/world/how-the-nsa-spies-on-international-bank-transactions-a-922430.html

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.7

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

In January 2014 the U.S. Justice Department adopted a policy allowing companies to report on national security letters and requests from the Foreign Intelligence Surveillance Court. The Department said, "the public interest in disclosing this information now outweighs the national security concerns that required its classification."8

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

Verizon, in publishing its first transparency report, said10:

"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."

Demands for confidential customer data are made by governments around the world. In February 2015, Twitter disclosed in a transparency report that total government requests for data rose by 40 percent compared to a previous report six months earlier. Twitter said the latest requests came from more than 50 countries.11

"These reports shine a light on government requests for customers' information," Jeremy Kessel, senior manager of global legal policy at Twitter, said in a company blog post. "Providing this insight is simply the right thing to do, especially in an age of increasing concerns about government surveillance."

Reports detailing government and law enforcement requests for confidential customer data are now also routinely published by Google12, Microsoft13, Facebook14, Yahoo!15, LinkedIn16, Apple17, Twitter18 and other consumer-facing Internet companies.

---

7 http://news.cnet.com/8301-1009_3-57603076-83/nsa-snoops-on-credit-card-transactions-says-report/
8 http://www.justice.gov/opa/pr/2014/January/14-ag-081.html
9 http://investorrelations.mastercardintl.com/phoenix.zhtml?c=148835&p=irol-Protection
10 http://publicpolicy.verizon.com/blog/entry/verizon-releases-first-transparency-report
11 http://bits.blogs.nytimes.com/2015/02/09/twitter-reports-surge-in-government-data-requests/?_r=0
12 https://www.google.com/transparencyreport/
13 http://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/
14 https://www.facebook.com/about/government_requests

15 http://info.yahoo.com/transparency-report/
16
http://blog.linkedin.com/2014/02/03/updated-linkedin-transparency-report-including-requests-related-to-u-s-national-security-r
17 http://images.apple.com/pr/pdf/140127upd_nat_sec_and_law_enf_orders.pdf
18 https://transparency.twitter.com/

Importantly, MasterCard has proactively responded to shareholder concerns by issuing a "Privacy & Data Protection" report.19 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, the focus of national and international lobbying campaigns, investigation by numerous non-governmental organizations, and an extraordinary amount of media attention.

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.

Target, one of America's largest retail chains, experienced breaches in 2013 that compromised the card accounts of an estimated 40 million customers and the personal information of as many 70 million people.20 In February 2015 Target disclosed that breach-related expenses not covered by insurance totaled $162 million; according to media reports, many experts believe the breach could continue to have a financial impact for years to come. American Express experienced a break in 2014, highlighted in the following section.

At a hearing on the Target breaches, Senator Patrick Leahy, of the Senate Judiciary Committee, said if consumers cannot trust businesses to keep their data secure, "our economic recovery is going to falter."21 [Proponent's emphasis]

In February 2012, the Obama Administration unveiled a "Consumer Privacy Bill of Rights"22 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."

---

19 http://investor.mastercard.com/investor-relations/corporate-goverance/policies-and-reports/default.aspx
20 http://www.marketwatch.com/story/targets-10-million-payout-to-consumers-is-tiny-part-of-its-data-breach-liability-2015-03-19
21 http://www.nytimes.com/2014/02/05/business/target-to-speed-adoption-of-european-anti-fraud-technology.html?hpw&rref=tec
22 http://www.whitehouse.gov/the-press-office/2012/02/23/fact-sheet-plan-protect-privacy-internet-age-adopting-consumer-priva

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.23 [Proponent's emphasis]

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."24 [Proponent's emphasis]

In May 2014, a working group appointed by President Obama to study Big Data and Privacy recommended the passage of federal data breach legislation. "Big data technologies make it possible to store significantly more data, and further derive intimate insights into a person's character, habits, preferences, and activities," said the working group's final report. "That makes the potential impacts of data breaches at businesses or other organizations even more serious." 25

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.26

---

24 http://www.whitehouse.gov/cybersecurity

2 5 http://energycommerce.house.gov/icymi/opinion-reps-marsha-blackburn-and-peter-welch-cnbc-congress-needs-take-action-dat

26 CF Disclosure Guidance: Topic No. 2, Cybersecurity, October 13, 2011.

Privacy and data security have attracted significant attention from leaders of the U.S. Congress. In 2015 Rep. Marsha Blackburn (R-TN) and Rep. Peter Welch (D-VT) introduced the bi-partisan Data Security and Breach Notification Act. “Hackers are stealing key personal data and cashing in on it at a staggering rate — tens of billions of dollars each year,” the Congress members said. “It's a modern day Wild West, and the descendants of Jesse James and the safe robbers of years past never had it so good. Too often, today's criminals don't even have a tough ‘safe’ to crack.”27

In January 2015, Sen. Patrick Leahy had said he would re-introduce 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.28 “The President’s new initiative on data breach notification is one piece of the necessary response to this serious problem, but we also need to make sure we protect consumer’s private information before breaches happen,” Sen Leahy said.29

A front page New York Times story (“As Hacking Against U.S. Rises, Experts Try to Pin Down Motive”30) 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.31

American Express recognizes the import and business implications of regulatory privacy risks in their 2014 10-k: 32

---

27 http://www.cnbc.com/id/102534111
28 http://blogs.wsj.com/riskandcompliance/2014/01/08/personal-data-privacy-bill-re-introduced-in-congress/
29 http://www.leahy.senate.gov/press/comment-of-senator-patrick-leahy-d-vt_ranking-member-senate-judiciary-committee--on-th
30 http://www.nytimes.com/2013/03/04/us/us-weighs-risks-and-motives-of-hacking-by-china-or-iran.html?hpw
31 https://www.sec.gov/Archives/edgar/data/4962/000119312514066777/d656045d10k.htm
32 https://www.sec.gov/Archives/edgar/data/4962/000119312515059931/d862737d10k.htm

Recent account data compromise events at large retailers, as well as the disclosure of the monitoring activities by certain governmental agencies, have resulted in heightened legislative and regulatory focus on privacy, data protection and information security around the world. Legislators and/or regulators in the United States and other countries in which we operate are increasingly adopting or revising privacy, data protection and information security 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. 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. [Proponents' 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 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.

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.

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

In May 2014, news media reported that "American Express is in the process of notifying 76,608 California residents that their credit card information was posted online back in March by an offshoot of the worldwide hacktivist collective Anonymous." American Express reportedly told the California Attorney General's office that it had informed customers of the following:

"At this time, we believe the recovered data may include your American Express Card account number, the card expiration date, the date your card became effective and the four digit code printed on the front of your card…Importantly, your Social Security number was not impacted and our systems have not detected any unauthorized activity on your card account related to this incident."

In April 2013, Advertising Age magazine reported33:

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.

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

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. 34

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.35

Conclusion:

The business, brand, and regulatory risks highlighted above 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.

---

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

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.

IMPORTANT NOTICE: The cost of this communication is being borne entirely by Arjuna Capital/Baldwin Brothers Inc. Arjuna Capital 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.