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

DIVISION OF
CORPORATION FINANCE

March 7, 2018

Tyler Mark
Bryan Cave LLP
tyler.mark@bryancave.com

Re: Express Scripts Holding Company
Incoming letter dated December 21, 2017

Dear Mr. Mark:

This letter is in response to your correspondence dated December 21, 2017 concerning the shareholder proposal (the "Proposal") submitted to Express Scripts Holding Company (the "Company") by the New York State Common Retirement Fund (the "Proponent") for inclusion in the Company's proxy materials for its upcoming annual meeting of security holders. We also have received correspondence on the Proponent's behalf dated January 16, 2018. Copies of all of the correspondence on which this response is based 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,

Matt S. McNair
Senior Special Counsel

Enclosure

cc: Cornish F. Hitchcock
Hitchcock Law Firm PLLC
conh@hitchlaw.com

March 7, 2018

Response of the Office of Chief Counsel
Division of Corporation Finance

Re: Express Scripts Holding Company
Incoming letter dated December 21, 2017

The Proposal asks the board to review and publicly report on its cyber risk and actions taken to mitigate that risk.

We are unable to conclude that the Company has met its burden of demonstrating that it may exclude the Proposal under rule 14a-8(i)(7) as a matter relating to the Company's ordinary business operations. Accordingly, we do not believe that the Company may omit the Proposal from its proxy materials in reliance on rule 14a-8(i)(7).

Sincerely,

Lisa Krestynick
Attorney-Adviser

DIVISION OF CORPORATION FINANCE
INFORMAL PROCEDURES REGARDING SHAREHOLDER PROPOSALS

The Division of Corporation Finance believes that its responsibility with respect to matters arising under Rule 14a-8 [17 CFR 240.14a-8], as with other matters under the proxy rules, is to aid those who must comply with the rule by offering informal advice and suggestions and to determine, initially, whether or not it may be appropriate in a particular matter to recommend enforcement action to the Commission. In connection with a shareholder proposal under Rule 14a-8, the Division's staff considers the information furnished to it by the company in support of its intention to exclude the proposal from the company's proxy materials, as well as any information furnished by the proponent or the proponent's representative.

Although Rule 14a-8(k) does not require any communications from shareholders to the Commission's staff, the staff will always consider information concerning alleged violations of the statutes and rules administered by the Commission, including arguments as to whether or not activities proposed to be taken would violate the statute or rule involved. The receipt by the staff of such information, however, should not be construed as changing the staff's informal procedures and proxy review into a formal or adversarial procedure.

It is important to note that the staff's no-action responses to Rule 14a-8(j) submissions reflect only informal views. The determinations reached in these no-action letters do not and cannot adjudicate the merits of a company's position with respect to the proposal. Only a court such as a U.S. District Court can decide whether a company is obligated to include shareholder proposals in its proxy materials. Accordingly, a discretionary determination not to recommend or take Commission enforcement action does not preclude a proponent, or any shareholder of a company, from pursuing any rights he or she may have against the company in court, should the company's management omit the proposal from the company's proxy materials.

HITCHCOCK LAW FIRM PLLC
5614 CONNECTICUT AVENUE, N.W. • NO. 304
WASHINGTON, D.C. 20015-2604
(202) 489-4813 • FAX: (202) 315-3552

CORNISH F. HITCHCOCK
E-MAIL: CONH@HITCHLAW.COM

16 January 2018

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

By electronic mail: shareholderproposals@sec.gov

Re: Shareholder proposal to Express Scripts Holding Company
from the New York State Common Retirement Fund

Dear Counsel:

I write on behalf of the New York State Common Retirement Fund (the "Fund") in response to the letter from counsel for Express Scripts Holding Company ("Express Scripts" or the "Company") dated 21 December 2017 (the "Letter") in which Express Scripts advises of its intent to omit the Fund's resolution (the "Resolution") from the Company's 2018 proxy materials. For the reasons set forth below, we respectfully ask the Division to deny the requested no-action relief.

The Resolution

Citing the current concerns about corporate cybersecurity, the Resolution asks the Board of Directors to:

> . . . review and publicly report (at reasonable cost, in a reasonable timeframe, and omitting proprietary and confidential information) on its cyber risk and actions taken to mitigate that risk.

The Resolution explains that a report adequate for investors to assess practices should include: aspects of business or operations that give rise to material cybersecurity risk; the extent to which the company outsources functions that have material cybersecurity risks, descriptions of those functions and how the company addresses those risks; a description of cyber incidents experienced by the company

that are individually or in the aggregate material, including a description of the costs and consequences; risks related to cyber incidents that remain undetected for an extended period; a description of relevant insurance coverage; compliance, regulatory or contractual obligations related to cyber risk; certification to widely recognized standards; and how cybersecurity risks are reflected in financial statements. The Resolution adds that the report should address the scope and frequency of the Board's oversight of cyber risks.

In seeking no-action relief, Express Scripts raises only one objection, namely, that the Resolution relates to the "ordinary business" of the Company and may thus be excluded under Rule 14a-8(i)(7). We explain below why Express Scripts has failed to carry its burden of showing that the Resolution may be excluded.

Discussion.

Express Scripts makes a detailed critique of the Fund's Resolution, citing a number of no-action letters on individual topics that have been held to involve a company's "ordinary business," *i.e.*, the Resolution deals with "procedures for protecting customer information," as well as legal and regulatory compliance, workplace practices and vendor contracts. In addition, we are told, the Fund's Resolution raises no "significant policy" issue that would allow shareholders to consider what might otherwise be considered a part of the Company's "ordinary business."

This critique misses an overriding point that answers all of these objections: The Resolution is about risk assessment, specifically, the risk that perhaps a single error by a single employee can cause significant damage to a company, its shareholders and millions, if not tens of millions, of individuals.

A proposal focusing on risk assessment can transcend "ordinary business" even if the proposal involves topics that, in another context, and without a significant risk factor, might warrant omission under the (i)(7) exclusion. In section B of STAFF LEGAL BULLETIN 14E (2009)[1] the Division advised that its approach to proposals on risk assessment would henceforth focus on–

> . . . whether the underlying subject matter of the risk evaluation involves a matter of ordinary business to the company. In those cases in which a proposal's underlying subject matter transcends the day-to-day business matters of the company and raises policy issues so significant that it would

[1] Express Scripts' letter advises (at p. 6) that the Company has not sought board input pursuant to the guidance recently issued in STAFF LEGAL BULLETIN 14I and is thus relying solely on the Division's prior guidance and no-action decisions.

> be appropriate for a shareholder vote, the proposal generally will not be excludable under Rule 14a-8(i)(7) as long as a sufficient nexus exists between the nature of the proposal and the company.

By any stretch of the imagination, the risks from inadequate cybersecurity measures transcend issues pertaining to employee relations, vendor contracts and other aspects that may in other situations be viewed as part of a company's "ordinary business."

We thus begin the discussion with a point that Express Scripts buries towards the end of its letter (at pp. 6-7), namely, the supposed lack of a "significant policy" component. If there is any doubt that cybersecurity is and should be a major concern of the Express Scripts board, consider this recent report from THE WALL STREET JOURNAL:

> As cybercriminals damage company reputations and cause tens of millions in remediation and legal costs, some boards are increasing cybersecurity oversight and weighing how to delegate responsibilities among directors. Others are pushing for more meetings with corporate security chiefs.
> . . .
> More than one in five directors say they are dissatisfied with the quality of cyber risk information that the board gets from management, according to a 2017 survey of 583 directors and executives with governance duties by the National Association of Corporate Directors. Those who feel confident the company they serve is properly secured against a cyberattack fell to 37% last year from 42% in 2016.

Nash, Lublin and Adriotis, *Boards Seek Bigger Role in Thwarting Hackers*, THE WALL STREET JOURNAL (10 January 2018), available at https://www.wsj.com/articles/boards-seek-bigger-role-in-thwarting-hackers-1515596400

In the discussion that follows we set forth a number of reasons why the Fund's Resolution raises significant policy issues. We focus on developments in the last 12 months.

A. <u>The Commission Declares Cybersecurity to be a Significant Issue.</u>

•On 26 September 2017, SEC Chairman Jay Clayton testified before the Senate Banking Committee:

> Cybersecurity is an area that is vitally important to the SEC, our markets and me personally. The prominence of this issue and the heightened focus

> the agency has on it is the result of various factors, including (1) the increased use of and dependence on data and electronic communications, (2) the greater complexity of technologies present in the financial marketplace and (3) the continually evolving threats from a variety of sources. Cybersecurity touches the daily lives of virtually all Americans, whether it is our accounts with financial services firms, the companies we invest in or the markets through which we trade.
> . . .
>
> Despite the attention given to widely-publicized cyber-related incidents experienced by the Commission and others, *I still am not confident that the Main Street investor has received a sufficient package of information from issuers, intermediaries and other market participants to understand the substantial risks resulting from cybersecurity and related issues. As a general matter, it is critical that investors be informed about the threats that issuers and other market participants face.*
>
> To be sure, we are continuing to examine whether public companies are taking appropriate action to inform investors, including after a breach has occurred, and we will investigate issuers that mislead investors about material cybersecurity risks or data breaches. As is noted in my July speech and on various other occasions, I would like to see more and better disclosure in this area (emphasis added).

Testimony on "Oversight of the U.S. Securities and Exchange Commission," available at https://www.sec.gov/news/testimony/testimony-clayton-2017-09-26.[2]

• In November 2017 Director William Hinman of the Division of Corporation Finance stated that the SEC may "refresh" existing staff guidance on what companies should be disclosing to their investors about cyberattacks – which of course is included within the subject matter of the Resolution. Ramonas, *SEC May 'Refresh' Cybersecurity Disclosure Guidance: Official*, BLOOMBERG, available at https://www.bna.com/sec-may-refresh-n73014471946/.

---

[2] Ironically, Chairman Clayton's testimony came only a few days after the Commission disclosed that a 2016 intrusion of the Commission's EDGAR test filing system may have provided the basis for illicit gain through trading. Press Release No. 2017-170, *SEC Chairman Clayton Issues Statement on Cybersecurity* (20 September 2017), available at https://www.sec.gov/news/press-release/2017-170. The following month the Senate Banking Committee considered two nominations to the Commission, and both Hester M. Peirce and Robert J. Jackson, Jr. identified cybersecurity as a top priority for the Commission. Ramonas, *SEC Should Focus on Cybersecurity, Nominees Say*, BLOOMBERG (25 October 2017), available at https://biglawbusiness.com/sec-should-focus-on-cybersecurity-nominees-say/

•In September 2017 the Commission announced new initiatives that build on the Division of Enforcement's ongoing efforts to address cyber-based threats and to protect retail investors. Press Release 2017-176, *SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors*, available at https://www.sec.gov/news/press-release/2017-176. In a speech highlighting the importance of cybersecurity to investors, the Division's Co-Director Stephanie Avakian gave a speech in which she spoke of:

> . . . the increasing frequency with which we are seeing cyber-related misconduct affecting the securities markets, and also the increasing complexity of these cases. These cybersecurity threats come from a wide range of sources, including foreign and domestic hackers, traders and others who traffic in stolen market-moving information, prospective market manipulators, state-sponsored actors, and others.
>
> . . . In an era where nearly every company is dependent on computer systems to operate their business, it is frequently necessary to provide meaningful and timely disclosures regarding cyber risks and incidents. These disclosures are often material on their own or necessary in order to make other disclosures, in light of the circumstances under which they are made, not misleading.

Speech, *The SEC Enforcement Division's Initiatives Regarding Retail Investor Protection and Cybersecurity* (26 October 2017), available at https://www.sec.gov/news/speech/speech-avakian-2017-10-26

•The Investor as Owner Subcommittee of the Commission's Investor Advisory Committee recently published a "Discussion Draft re: Cybersecurity and Risk Disclosure," available at https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwiksp6mst3YAhUFUt8KHUq_BaMQFgg1MAI&url=https%3A%2F%2Fwww.sec.gov%2Fspotlight%2Finvestor-advisory-committee-2012%2Fdiscussion-draft-cybersecurity-disclosure-iac-120717.pdf&usg=AOvVaw1StbkZPDAjvhu2mecZLD73. This document has not been approved by the Subcommittee and, we understand, may be revised prior to its presentation to the full Investor Advisory Committee, probably in March 2018. Nonetheless we cite this draft for its compilation and discussion of studies and factual information from public sources, including:

•A 2017 study by IBM concluding that each data break on average will compromise 24,089 confidential records and cost a company's shareholders $4 million.

•A December 2016 survey by the National Association of Corporate Directors in which only 19 percent of the 600 directors surveyed said that their boards have "a

high level of understanding" of cybersecurity risks.

B. Congress Considers Legislative Solutions to Cybersecurity Risks.

A useful indicium of policy significance is Congressional interest in a topic. During the current Congress nearly 200 bills relating to cybersecurity have been introduced,[3] including:

• S. 536, the Cybersecurity Disclosure Act of 2017, by Sens. Reed (D-RI) and Collins (R-ME), to require that if a corporate board does not include a cybersecurity expert, the SEC should require an explanation of the process that went into the selection process.

• H.R. 4668, the Small Business Advanced Cybersecurity Enhancements Act of 2017, by Rep. Chabot (R-OH), to provide for the establishment of an enhanced cybersecurity assistance and protections for small businesses, and for other purposes.

• S. 2179, the Data Security and Breach Notification Act, by Sen. Nelson (D-FL), to require reasonable security policies and procedures to protect data containing personal information, and to provide for nationwide notice in the event of a breach of security.

• H.R.4028, the PROTECT Act, by Rep. McHenry (R-NC), to establish cybersecurity supervision and examination of large consumer reporting agencies, and for other purposes.

• H.R. 4053, by Rep. Fortenberry (R-NE), to amend the Fair Credit Reporting Act to require an independent audit of the cybersecurity practices of certain consumer reporting agencies, and for other purposes.

• S.2124, the Consumer Privacy Protection Act, by Sen. Leahy (D-VT), to require companies with sensitive consumer information, such as Equifax, to maintain safeguards to ensure the privacy and security of such data, and to notify consumers when that sensitive data is breached.

C. The Equifax Breach

In September 2017 Equifax, a major credit reporting agency, reported that attackers had found a flaw in its website that was used to obtain personal information of as many as 145 million Americans. The stolen data included names, Social Security numbers, birth dates, addresses and driver's license numbers. The breach resulted in investigations by and demands from all 50 attorneys general, the

[3] This calculation is based on a search for "cybersecurity" at Congress.gov for bills introduced with that word in the 115th Congress. See https://www.congress.gov/search?searchResultViewType=expanded&pageSort=dateOfIntroduction%3Adesc&q=%7B%22source%22%3A%22legislation%22%2C%22search%22%3A%22cybersecurity%22%2C%22congress%22%3A%22115%22%7D

SEC, the Justice Department, Federal Trade Commission, the Consumer Financial Protection Bureau, and regulators in Britain and Canada. By early November the company estimated that the breach resulted in costs of $87 million—and climbing. Quarterly profits dropped 27 percent from a year earlier, and some corporate customers expressed skittishness about dealing with Equifax until the company could assure customers that the systems are secure. Cowley, *Equifax Faces Mounting Costs and Investigations From Breach*, THE NEW YORK TIMES (9 November 2017), available at https://www.nytimes.com/2017/11/09/business/equifax-data-breach.html

D. The Risk is Acute in the Health Care Sector.

The discussion thus far has demonstrated that cybersecurity is a "significant policy" issue and a topic of legitimate concern among investors. That significance and the presence of cyber risk are particularly pronounced as to companies in the healthcare industry, such as Express Scripts, which are subject to stringent federal requirements regarding the security of patient information.

The Ponemon Institute, which conducts independent research on privacy, data protection and information security policy, issues an annual report on privacy and security of health care information. In reporting on the 2016 results of its survey of health care organizations, including companies such as Express Scripts, the Institute stated:

> **Healthcare organizations and business associates believe they are more vulnerable than other industries to a data breach.** An overwhelming majority of healthcare organizations (69 percent) and business associates (63 percent) believe they are at greater risk than other industries for a data breach. The top reasons for healthcare organizations are a lack of vigilance in ensuring their partners and other third parties protect patient information (51 percent) and not enough skilled IT security practitioners (44 percent). In contrast, business associates say their vulnerabilities are due to employees' negligence in handling patient information (54 percent) and a lack of technologies to mitigate a data breach (50 percent).
>
> **Recent well-publicized data breaches in healthcare have put the industry on alert.** Sixty seven percent of healthcare organizations and 62 percent of business associates say these data breaches affected their security practices. Both types of organizations are taking the same steps: more vigilance in ensuring their partners and other third parties safeguard patient information, more investments in technologies to mitigate a data breach and increased employee training.

Ponemon Institute, *Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data* , p 4, (16 May 2016), available at https://www.ponemon.org/library/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data-1.[4]

Despite the nature of these risks, Express Scripts provides little information of value to investors, hence this Resolution. The Company's most recent Form 10-K (filed 14 February 2017) treats the issue in a cursory manner. "Security breaches including cyber attacks" are listed (at p. 20) as part of a laundry list of items that could "incur disruptions to our business operations or negative impacts to patient safety, customer and member disputes, damage to our reputation, exposures to risk of loss, litigation or regulatory violations, increased administrative expenses or other adverse consequences." Further details are not provided.

Apart from these concerns, there is a separate source of risk. Until recently, lawsuits based on a data breach were difficult to maintain and were susceptible to dismissal at an early stage, given that it can be challenging for consumers to show that they suffered financial harm or injuries connected to a specific incident.

That appears to be changing, however. According to a recent report in THE WALL STREET JOURNAL, "U.S. federal judges have seemed to change course in the past year, allowing several cases to proceed following companies' motions to dismiss." The two cited cases involve companies in the health care field, Horizon Healthcare Services and CareFirst. A former head of the Federal Communications Commission's Enforcement Bureau cited as reasons for the shift: "Breaches are getting more frequent and larger, and there's a need to have more accountability and for the judicial process to ensure there's accountability." Janofsky, *Why Companies Should Prepare for More Data Breach Lawsuits*, THE WALL STREET JOURNAL (11 December 2017), available at https://www.wsj.com/articles/why-

[4] This survey includes 91 companies that are "covered entities" as defined by patient privacy regulations issued under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), *i.e.*, (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which the Department of Health and Human Services has adopted standards. The survey includes 84 "business associates" or "BAs" of these entities, which provide services or activities to a covered entity that involve the use or disclosure of individually identifiable health information. *Id.* at 2.

Express Scripts has acknowledged its obligations under HIPAA regulations as a "business associate" and perhaps as a "covered entity." In a document entitled *General HIPAA Implementation FAQ*, www.reachfastmd.com/Resources/Pdfs/hipaaFAQ.pdf, The Company asks (at p. 3) "What are Express Scripts' obligations under HIPAA?" The answer notes that the Company's "mail service and Specialty Distribution Services (SDS) may be covered entities in their capacity as health care providers" and that its "Pharmacy Benefit Management" ("PBM") business serves as a business associate and trading partner of many covered entities.

companies-should-prepare-for-more-data-breach-lawsuits-1512563334

Three Stanford University business professors recently highlighted some of the risks in this area in a paper calling for greater cybersecurity expertise in the boardroom. Larcker, Reiss and Tayan, *Critical Update Needed: Cybersecurity Expertise in the Boardroom*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE AND FINANCIAL REGULATION (12 December 2017), available at https://corpgov.law.harvard.edu/2017/12/12/critical-update-needed-cybersecurity-expertise-in-the-boardroom/. Their paper studied data breaches over the past five years and made several findings of relevance here:

• "[C]ompanies and their supply chains have been compromised by ransomware attacks in which cybercriminals disrupt computing systems or demand payment under threat of disrupting systems"; for example, a malware attack in July 2017 "took down the computing systems of major multinational corporations — such as Merck, Mondelez and Maersk—and disrupted operations for multiple days.

• Another target is "corporate networks or employee devices that store the personal information of clients and employees." Health insurance networks such as Anthem, Primera, and CareFirst BlueCross have been targeted by cybercriminals who steal the names, birthdays, addresses, social security numbers and health information of customers."

• Exhibit 3 of that report summarizes the multi-million dollar costs of recent settlements of class actions lawsuits alleging data theft, including theft of health and personal information. Some settlements involve well-known breaches at Target and Home Depot, but the payouts extend to some less well-known names in the health care field, namely, St. Joseph Health System, CBR Systems and AvMed.

E. <u>The No-Action Decisions Cited by the Company Are Unpersuasive.</u>

Notwithstanding these significant developments over the past 12 months, Express Scripts maintains that we are not dealing with anything out of the ordinary – certainly nothing about which shareholders are entitled to have a say. The Company's arguments, however, fall short of establishing that point, and the no-action decisions they cite involve different situations. We take each point in turn.

1. The Resolution Focuses on Policies and Procedures Relating to Privacy of Customers and Other Third Parties and Data Management. Letter at pp. 3–4.

Express Scripts cites two proposals requesting reports on a company's policies for protecting customer and user privacy and another company's

implementation of various commitments to privacy and data security. *See AT&T Inc.* (Feb. 5, 2016); *Verizon Communications Inc.* (Feb. 16, 2017). Express Scripts notes that the Division excluded the proposal because it was deemed to relate to "procedures for protecting customer information" and, in the case of the *AT&T* letter, did "not focus on a significant policy issue."

As we have just explained, however, much has changed since the *AT&T* letter. Indeed, it would be fair to characterize the Equifax breach itself as a watershed moment, affecting 143 million people.

Moreover, the two proposals covered more—and different—ground than the Fund's Resolution here. The *Verizon* proposal sought a report on Verizon's "progress towards implementing its various commitments pertaining to privacy, free expression and data security," including the company's privacy policies, human rights privacy and broadband commitment policy. We acknowledge that the supporting statement in particular focused on data security, specifically with reference to Verizon's acquisition of Yahoo!, which had a significant data breach issue in 2014. Although that single event would not have been enough to sway the Division as to the Verizon proposal, we submit that enough additional information is now available to tip the balance towards finding that the Fund's Resolution raises a "significant policy" issue. For these reasons as well, we submit that cited letters prior to 2016, if not distinguishable on the facts, do not address the risk to companies and investors as they are known, and acknowledged by Congress, the SEC, investors and the general public, today.

The AT&T proposal that Express Scripts cites did not deal even remotely with cybersecurity, but rather the separate issue of telecoms companies providing "information to law enforcement and intelligence agencies, domestically and internationally, above and beyond what is legally required by court order or other legally mandated process." To the same effect is *AT&T Inc.* (30 January 2017) (agreeing as to a request for a report regarding disclosure of customer communications and related information to law enforcement officials).

2. *The Resolution is about "legal and regulatory compliance."* Letter at pp. 4–5.

Not so. Express Scripts is certainly correct that the Division has concurred with respect to proposals requesting little more than something such as a report on a company's "compliance with state and federal employment and labor laws." *E.g., FedEx Corp.* (14 July 2009). The resolution does not request information about the Company's compliance; it *requests* information about its legal and contractual *obligations*. As we noted at the outset, the Resolution is about risk assessment. It is

not about compliance matters at all. The Company appears to construe legal and regulatory matters far too broadly here. If anything, the Company appears to acknowledge that the "type of information" being requested is not "routine" and that the topic of this Resolution deals with an overarching policy issue.

3. *The Resolution "attempts to micro-manage Express Scripts' management of its workplace practices."* Letter at p. 5.

As a practical matter, one cannot talk about or tackle cybersecurity issues without talking about a company's workforce and workforce training. Consider, for example, how the Equifax breach was the result of a single employee failing to take the requisite remedial steps at the proper time. Bernard and Cowley, *Equifax Breach Caused by Lone Employee's Error, Former CEO Says,* THE NEW YORK TIMES (3 October 2017), available at https://www.nytimes.com/2017/10/03/business/equifax-congress-data-breach.html.

Although it is true that ultimately cybersecurity is a matter of systems management, systems are managed by people, and the human element cannot be ignored. Indeed, accounts in the media show that it is very easy for a company's security to be breached if (as at Boeing) an employee emails a spouse for help formatting a document or (as at Snapchat) the hacker pretended to be the CEO and persuaded an employee to e-mail personal information on hundreds of employees.[5]

That is why, for example, a federal inter-agency task force report on "best practices" to prevent ransomware, after noting that "[o]n average, more than 4,000 ransomware attacks have occurred daily since January 1, 2016," contained as its principal recommendation: "Educate Your Personnel" in several ways. *How to Protect Your Networks from Ransomware*, pp. 2, 3, available at https://www.justice.gov/criminal-ccips/file/872771/download. Others who advise companies on the importance of effective cybersecurity measures emphasize the importance of educating a workforce and of being vigilant as to possible exposure from everyday occurrences, such as a lost or misplaced laptop or the vulnerability of tax and W-2 information.[6]

---

[5] McIntosh, *Boeing discloses 36,000-employee data breach after email to spouse for help*, PUGET SOUND BUSINESS JOURNAL (28 February 2017), available at https://www.bizjournals.com/seattle/news/2017/02/28/boeing-discloses-36-000-employee-data-breach.html; Peterson, *The human problem at the heart of Snapchat's employee data breach*, THE WASHINGTON POST (1 March 2016), available at https://www.washingtonpost.com/news/the-switch/wp/2016/03/01/the-human-problem-at-the-heart-of-snapchats-employee-data-breach/?utm_term=.71b17dea90c9

[6] These examples are taken from a series of articles that the Bryan Cave law firm has posted online advising potential corporate clients on *How Employers Can become Experts at Data Breaches*. See

The 2016 survey by the Ponemon Institute, cited above, confirms the importance of this issue (at p. 4):

> **Employee negligence continues to be the greatest concern.** When healthcare organizations were asked what type of security incident worries them most, by far it was the negligent or careless employee (69 percent of respondents). Forty-five percent of respondents said it was cyber attackers and 30 percent said it is the use of insecure mobile devices. These findings are virtually unchanged since 2015.
>
> The research found that many healthcare organizations and their business associates are negligent in the handling of patient information. While external threats dominate, internal problems such as mistakes — unintentional employee actions, third-party snafus, and stolen computing devices—are equally a problem and account for a significant percentage of data breaches. *In fact, 36 percent of healthcare organizations and 55 percent of BAs named unintentional employee action as a breach cause* (emphasis added).

4. *The Resolution deals with "vendor and third-party contractual relationships."* Letter at 5-6.

Express Scripts next cites to letters concurring the view that a company may omit "decisions relating to vendor relationships" or "the manner in which the company monitors the conduct of its suppliers and their subcontractors," citing *Continental Airlines, Inc.* (25 March 2009). *Continental Airlines*, however, involved a repair station run by a contractor hired by the airline, and apart from general references to air safety concerns, no overriding policy issue was implicated.

Here, by contrast, we deal with an issue of a different magnitude. A company such as Express Scripts is part of a chain that moves prescription drugs from the point of manufacture through a number of intermediaries, including the Company's pharmacy benefits management (or "PBM") business, until the product reaches the ultimate consumer. A breach anywhere in the chain can have devastating effects.

---

https://www.bryancave.com/images/content/1/7/v2/1745/SEC-Cybersecurity-Guidev4.pdf; https://www.bryancave.com/en/thought-leadership/how-employers-can-become-experts-at-data-breaches-lost-laptops.html; https://www.bryancave.com/en/thought-leadership/how-employers-can-become-experts-at-data-breaches-tax-and-w2.html; https://www.bryancave.com/en/thought-leadership/how-employers-can-become-experts-at-data-breaches-retaining-a.html; https://www.bryancave.com/en/thought-leadership/how-employers-can-become-experts-at-data-breaches-creating-an.html

The inter-connectedness of this network is one reason why, as the Ponemon Institute indicates (at p. 8, supra), the Department of Health and Human Services seeks to protect patient privacy by applying HIPAA rules not simply to "covered entities" that provide care directly to patients, but also to the "business associates" of these entities, a category that Express Scripts concedes includes the Company's PBM business. As noted by the Stanford business professors' paper (supra, at p. 9): "companies *and their supply chains* have been compromised" by ransomware attacks (emphasis added).

Thus, whatever conclusion one may draw about the nature of "vendor relationships" in other industries or in other contexts, those concerns are not salient when, as here, we deal with a complex supply chain in which a single breach at any point in the chain can result in significant negative effects up or down the line.

Conclusion.

Express Scripts has thus failed to carry its burden of showing that the Resolution may be excluded because it addresses the "ordinary business" of the Company. Accordingly, we respectfully ask you to advise Express Scripts that the Division cannot concur with the Company's objections.

Thank you for your consideration of these points. Please feel free to contact me if any additional information would be helpful.

Very truly yours,

Cornish F. Hitchcock

Cornish F. Hitchcock

cc: Tyler Mack, Esq.

BRYAN CAVE

BRYAN CAVE LLP 1700 Lincoln Street, Suite 4100, Denver, CO 80203-4541
T: 303 861 7000 F: 303 866 0200 bryancave.com

December 21, 2017

Tyler Mark
Direct: 303/866-0238
Fax: 303/335-3838
tyler.mark@bryancave.com

Securities Exchange Act of 1934 / Rule 14a-8

VIA E-MAIL (shareholderproposals@sec.gov)

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

Re: 2018 Express Scripts Holding Company Annual Meeting of Stockholders - Notice of Intent to Omit Stockholder Proposal Submitted by the New York State Common Retirement Fund Pursuant to Rule 14a-8

Ladies and Gentlemen:

Pursuant to Rule 14a-8(j) of the Securities Exchange Act of 1934, as amended (the "Exchange Act"), our client, Express Scripts Holding Company, a Delaware corporation ("Express Scripts" or the "Company"), hereby notifies the Staff of the Division of Corporation Finance (the "Staff") of the Securities and Exchange Commission (the "Commission") of its intention to exclude a shareholder proposal (the "Proposal") submitted by the Comptroller of the State of New York on behalf of the New York State Common Retirement Fund (the "Proponent") from Express Scripts' proxy materials for its 2018 Annual Meeting of Stockholders (the "2018 Proxy Materials") for the reasons stated below. The Company requests confirmation that the Staff will not recommend any enforcement action if the Company omits the Proposal from the 2018 Proxy Materials for the reasons detailed below.

This letter, together with the Proposal and the related correspondence, are being submitted to the Staff via e-mail in lieu of mailing paper copies. In accordance with Rule 14a-8(j), this letter is being submitted more than 80 calendar days before the date on which the Company expects to file the definitive 2018 Proxy Materials. A copy of this letter and the attachments are being sent on this date to the Proponent advising of Express Scripts' intention to omit the Proposal from its 2018 Proxy Materials. We respectfully remind the Proponent that if the Proponent elects to submit additional correspondence to the Commission or the Staff with respect to the Proposal, a copy of that correspondence should be furnished concurrently to the undersigned pursuant to Rule 14a-8(k).

I. The Proposal

The Proposal includes the following resolution:

> RESOLVED: The Company's shareholders ask the Board to review and publicly report (at reasonable cost, in a reasonable timeframe, and omitting proprietary and confidential information) on its cyber risk and actions taken to mitigate that risk. A report adequate for investors to assess practices should include:

aspects of business or operations that give rise to material cyber risk;

the extent to which the Company outsources functions that have material cyber risks, descriptions of those functions and how the Company addresses those risks;

descriptions of cyber incidents experienced by the Company that individually or in the aggregate are material, including a description of costs and consequences;

risks related to cyber incidents that remain undetected for an extended period;

description of relevant insurance coverage;

compliance, regulatory or contractual obligations related to cyber risk;

certification to widely recognized standards; and

how cyber risks and cyber incidents are reflected in financial statements.

The report should also discuss the scope and frequency of the Board's oversight of cyber risks which may include review of relevant systems, policies, and procedures, related to:

- determining critical assets (e.g., customer information);
- employee training on data security and privacy-related risks;
- due diligence for third party vendors and potential acquisitions;
- data breach and incident response plans;
- minimization of data collection and retention; and
- security policies and audit frequency

A copy of the Proposal, together with the Proponent's supporting materials and related correspondence are attached to this letter as Exhibit A.

II. The Company May Exclude the Proposal Pursuant to Rule 14a-8(i)(7) Because the Proposal Focuses on Matters of Ordinary Business.

The Company believes that the Proposal may be properly excluded from the 2018 Proxy Materials pursuant to Rule 14a-8(i)(7), which permits a company to omit a shareholder proposal from its proxy materials if the proposal deals with a matter relating to the company's "ordinary business operations." The purpose 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." Release No. 34-40018 (May 21, 1998) (the "1998 Release"). Two considerations underlie this exclusion. The first relates to the subject matter of the proposal: "[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.* The second consideration relates to the "degree to which the proposal seeks to 'micro-manage' the company by probing too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." *Id.*

In applying Rule 14a-8(i)(7) to proposals requesting companies to prepare reports on specific aspects of their business, the Staff has determined that it will consider whether the subject matter of the report involves a matter of ordinary business. If it does, the proposal can be excluded even if it requests only the preparation of the report and not the taking of any action with respect to such ordinary business matter. Release No. 34-20091 (Aug. 16, 1983). Similarly, the Staff indicated in Staff 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. *See, e.g.*, *Sempra Energy* (Jan. 12, 2012, *recon. denied* Jan. 23, 2012) (concurring in the exclusion of the proposal and noting 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"). As discussed in greater detail below, the main focus of the Proposal, as well as each separate aspect of this Proposal, addresses particular business risks and internal policies and procedures that, in each instance, constitute ordinary business matters for the Company.

The Proposal Focuses on Policies and Procedures Relating to Privacy of Customers and Other Third Parties and Data Management

The Proposal can be excluded under Rule 14a-8(i)(7) because it focuses on the Company's policies and procedures for protecting the data and privacy of customers and other third parties. The Staff has repeatedly recognized that the protection of customer and other third party data and privacy is a core management function not subject to shareholder oversight. In fact, in the last two years the Staff concurred in the exclusion of proposals asking for reports on (i) one company's policies for protecting customer and user privacy and (ii) another company's implementation of various commitments to privacy and data security. *See AT&T Inc.* (Feb. 5, 2016); *Verizon Communications Inc.* (Feb. 16, 2017). In each case, the Staff issued a no-action letter stating it would not object if the company excluded the proposal on the grounds that the proposal "relates to procedures for protecting customer information" and noted in particular with respect to the proposal received by AT&T in the 2016 proxy season that the proposal "does not focus on a significant policy issue." The Staff has taken a similar position in numerous other instances. *See, e.g.*, *Bank of America Corp.* (Feb. 21, 2006) (concurring in the exclusion of a proposal seeking a report on policies and procedures for ensuring that all personal and private information of company customers would remain confidential); *AT&T Inc.* (Feb. 9, 2007) (concurring in the exclusion of a proposal seeking a report regarding disclosure of customer communications and related information to specified governmental agencies); *AT&T Inc.* (Jan. 26, 2009) (concurring in the exclusion of a proposal seeking a report addressing privacy and free expression in the context of internet providers); *Comcast Corporation* (Mar. 4, 2009) (concurring in the exclusion of a proposal seeking a report concerning data security and privacy issues related to the company's internet network management practices); *AT&T Inc.* (Jan. 30, 2017) (concurring in the exclusion of a proposal seeking a report regarding disclosure of customer communications and related information to law enforcement officials).

This analysis applies broadly, not only to issues concerning data security and customer privacy, but generally to a company's policies and procedures relating to data management and the handling of company accounts. Particularly instructive is *Huntington Bancshares Inc.* (Jan. 10, 2011), where the Staff concurred in the exclusion of a proposal concerning minimum retention standards for electronic files and the adoption of

internal controls to "safeguard [company] assets from unauthorized access and accidental loss or deletion." The Staff noted specifically that the proposal "relates to the policies and procedures for the retention of records regarding the products and services [the company] offers."

This Proposal focuses squarely on the details of the Company's policies and procedures relating to the protection of customer and other third party information and day-to-day data management. The resolution itself expressly focuses on a "cyber risk" report that is required or suggested to include disclosure on numerous aspects of the business relating to the privacy of customers and third parties and data management, including:

- the Company's privacy and data management operations and other "aspects of business or operations that give rise to material cyber risk";
- "compliance, regulatory or contractual obligations related to cyber risk," which implicate the Company's data management systems, privacy protection practices, and customer relationships;
- "systems, policies, and procedures" specific to protecting "patient data" and "critical assets, (e.g., customer information)";
- "training on data security and privacy-related risks";
- particulars with respect to systems, policies, and procedures concerning the Company's broader data management practices (e.g., "data breach and incident response plans" and the "minimization of data collection and retention"); and
- the Company's "security policies" themselves.

The supporting materials also focus on concerns regarding the protection of customer and other third-party information and day-to-day data management, including:

- "cyber incidents resulting in data breaches";
- "data breaches in healthcare" that put "patient data at risk"; and
- a data breach from 2008 "affecting personal and medical information of over 700,000 customers."

In all, the Proposal focuses so clearly on issues and disclosures related to the Company's policies and procedures concerning the privacy of customers and third parties and data management practices that it makes reference to these issues and requested disclosures a dozen or more times in the span of its twelve sentences. As noted above, whether in the context of a risk assessment or otherwise, these are precisely the types of day-to-day business practices that the Staff has consistently viewed as matters of ordinary business.

The Proposal Also Addresses Other Ordinary Business Matters

The Proposal also addresses a number of other matters relating to the Company's ordinary business operations, such as legal and regulatory compliance, workplace practices and employee management, and vendor and other third-party contractual relationships, each of which constitutes an ordinary business matter for the Company.

Legal and Regulatory Compliance

The Staff has long viewed a company's compliance with laws and regulations as a matter of ordinary

business. *See, e.g.*, *Navient Corporation* (Mar. 25, 2015) (concurring with exclusion of a proposal calling for a report on the company's internal controls over its student loan servicing operations and stating that "[p]roposals that concern a company's legal compliance program are generally excludable under rule 14a-8(i)(7)"). *See also FedEx Corp.* (Jul. 14, 2009) (concurring in the exclusion of a proposal calling for the board to establish an independent committee to prepare a report that discussed compliance with state and federal employment and labor laws). This Proposal requests the Company to review, and report on, the Company's legal and regulatory compliance program relating to its data management practices and its procedures and processes for protecting the information of customers and other third parties. It expressly calls for disclosures concerning "compliance [and] regulatory" obligations, "audit frequency" and any "certifications to widely recognized standards." This type of information cannot be separated out from the routine legal and regulatory compliance programs the Company has in place relating to its cyber security systems, data management, customer privacy policies, and general risk management practices and should therefore be excluded in reliance on Rule 14a-8(i)(7).

Workplace Practices and Employee Management

The Proposal is also excludable as relating to the Company's ordinary business operations because it attempts to micro-manage Express Scripts' management of its workplace practices. Specifically, the Proposal goes beyond merely asking for high-level information on cyber security-related risks and instead delves into the granular operational details of the Company's workplace management practices by calling for the board to report on its oversight of any "relevant systems, policies, and procedures related to… employee training" as it pertains to cyber security matters. The Staff has clearly and consistently articulated that "[p]roposals concerning a company's management of its workforce are generally excludable under rule 14a-8(i)(7)." *Starwood Hotels & Resorts Worldwide, Inc.* (Feb, 14, 2012). In *United Technologies* (Feb. 19, 1993), the Staff stated the following with respect to the predecessor rule to Rule 14a-8(i)(7) in addressing policies and procedures relating to general workplace management: "As a general rule the staff views proposals directed at a company's employment policies and practices with respect to its non-executive workforce to be *uniquely matters relating to the conduct of the company's ordinary business operations*. Examples of the categories of proposals that have been deemed to be excludable on this basis are: employee health benefits, general compensation issues not focused on senior executives, *management of the workplace*, *employee supervision*, labor-management relations, employee hiring and firing, conditions of the employment and *employee training* and motivation." (Emphasis added.)

The success of the Company's business is, of course, linked in part to management's ability to properly develop, manage, supervise and maintain "systems, policies, and procedures" to train its employees to ensure the security and integrity of any and all customer and third-party data held by the Company. In that light, dozens of employee training-related "systems, policies, and procedures," ranging from risk management training to ethics, conflict of interest and other policies and practices concerning employees, are implicated by such a request. As a result, the Proposal would conflict with the Staff's long-standing view that the general administration of a company's internal operating policies and practices, including the terms of such policies and practices, are part of a company's ordinary business operations. As such, the Proposal "prob[es] too deeply into matters of a complex nature upon which shareholders, as a group, would not be in a position to make an informed judgment." 1998 Release.

Vendor and Other Third-Party Contractual Relationships

The Staff also permits the exclusion of proposals concerning "decisions relating to vendor

relationships" or "the manner in which the company monitors the conduct of its suppliers and their subcontractors." *See Continental Airlines, Inc.* (Mar. 25, 2009) (concurring in the exclusion of a proposal requesting that the company adopt a policy applicable to all domestic and foreign contract repair facilities, noting that it related to the company's "ordinary business operations (i.e., decisions relating to vendor relationships)"); and *Foot Locker, Inc.* (Mar. 3, 2017) (concurring in the exclusion of a proposal concerning the monitoring of compliance with corporate codes by vendors and their subcontractors and the processes and procedures the company had in place for dealing with non-compliance), respectively. *See also Alaska Air Group, Inc.* (Mar. 8, 2010) (concurring in the exclusion of a proposal that requested a report discussing the maintenance and security standards used by the company's aircraft contract repair stations and the company's procedures for overseeing maintenance performed by the contract repair stations); and *Dean Foods Co.* (Mar. 9, 2007) (concurring in the exclusion of a proposal that requested an independent committee review of the company's standards for organic dairy product suppliers). This is the substantive core of the Proposal's specific request that the Company provide disclosures regarding "relevant systems, policies, and procedures related to… due diligence for third party vendors and potential acquisitions," "the extent to which the Company outsources functions that have material cyber risks, descriptions of those functions and how the Company addresses those risks," and "description[s] of relevant insurance coverage." These requests delve into both the substance of the Company's third-party relationships as well as the mechanical procedures used by the Company to evaluate potential vendors and monitor compliance with the Company's policies vis-à-vis cyber security risks. As such, the Proposal implicates, in yet another significant way, the day-to-day oversight and operation of the business by the board and management and is therefore subject, in yet another respect, to the ordinary business exclusion provided under Rule 14a-9(i)(7).

The Proposal Does Not Focus on a Significant Policy Issue.

Finally, the Proposal does not raise a significant policy issue. The Commission has stated that "proposals relating to such [ordinary business] matters but focusing on sufficiently significant social policy issues (e.g., significant discrimination matters) generally would not be considered to be excludable because the proposals would transcend day-to-day business matters and raise policy matters so significant that it would be appropriate for a shareholder vote." 1998 Release. In this case, the core issue raised by the Proposal is clearly the Company's policies and procedures relating to data management and the protection of customer and other third party privacy, which constitute matters of ordinary business. Moreover, in both its substance and practical application, the Proposal also implicates numerous other well-established bases for exclusion under Rule 14a-8(i)(7) for the reasons addressed above, whether relating to (i) the operation of the Company's compliance programs, (ii) the training of the Company's workforce, or (iii) the Company's contractual relationships with its vendors and other third parties. In each of these particular aspects, the Proposal focuses on matters of ordinary business and fails to raise a significant social policy issue. The Company notes that the Staff has provided guidance concerning the role a company's board could play in determining whether a proposal focuses on significant policy issues. Staff Legal Bulletin 14I (Nov. 1, 2017). In our case, however, we believe the Board's input is unnecessary because the Proposal falls within this long line of precedent no-action correspondence clearly establishing the basis for the exclusion.

As recognized in the Staff positions discussed above, overseeing and managing cyber security risk, while vital for most modern businesses and an important function of management and the board, is not a significant policy issue. Instead, these are technical and commercial issues. Due to the nature of Express Scripts' business, its core day-to-day operations inherently involve collecting, managing, and protecting sensitive data

from customers, patients and other third parties. In addition to the customers and patients, the Company's data management systems store confidential data and information from sellers, suppliers, and other service providers. The Company uses multiple methods and processes to protect privacy and secure data, many of which require some level of confidentiality and might otherwise be undermined or compromised by the type of disclosures contemplated in the Proposal. The board's and management's oversight of these data security methods and processes is, therefore, a central aspect of the day-to-day management and oversight of 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. The particulars involved in implementing and overseeing these policies, procedures, and tasks are central management functions. These are not policy issues that "transcend the day-to-day business matters" of the Company but issues "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.

The Proponent, no doubt, shares the concerns of many of the Company's stockholders about the emerging risks related to cyber security generally; however, overseeing and implementing policies and procedures relating to data management and the protection of customer and other third party privacy as well as managing the day-to-day mechanics of those policies and procedures are not, in themselves, sufficiently significant policy issues. The Staff has concluded as recently as earlier this year these are matters of ordinary business operations. *See, e.g., AT&T Inc.* (Jan. 30, 2017) *supra.* There is no reason for the Staff to change its view today. The Company, therefore, believes that it may properly exclude the Proposal from its 2018 Proxy Materials in reliance on Rule 14a-8(i)(7).

III. Conclusion

Based on the foregoing analysis, we respectfully request the Staff concur that it will take no action if Company excludes the Proposal from its 2018 Proxy Materials in reliance on Rule 14a-8. We would be happy to provide you with any additional information and answer any questions that you may have regarding this subject. If the Staff is unable to agree with our conclusions without additional information or discussions, we respectfully request the opportunity to confer with members of the Staff prior to issuance of any written response to this letter. Correspondence regarding this letter should be sent to me at tyler.mark@bryancave.com. If I can be of any further assistance in this matter, please do not hesitate to contact me at (303) 866-0238 or my colleague Taavi Annus at (314) 259-2037.

Sincerely,

Tyler Mark

Attachments

cc: Martin P. Akins, Senior Vice President, General Counsel, Express Scripts Holdings Company
Nick H. Varsam, Vice President & Associate General Counsel, Express Scripts Holdings Company
Taavi Annus, Partner, Bryan Cave LLP

Thomas P. DiNapoli, Comptroller of the State of New York
Gianna McCarthy, Director of Corporate Governance, Office of Comptroller of the State of New York

Exhibit A

Mark, Tyler

Subject: FW: Shareholder Request

From: TGoldsmith@osc.state.ny.us [mailto:TGoldsmith@osc.state.ny.us]
Sent: Wednesday, November 15, 2017 3:25 PM
To: Akins, Martin (EHQ)
Subject: [EXTERNAL] Shareholder Request

Hello Mr. Akins,

Please find attached a copy of the New York State Common Retirement Fund filing letter and shareholder resolution, which has also been sent to you today via UPS.

If you have any questions, please feel free to contact me regarding this transmission.

Kind Regards,

Tana

Tana Goldsmith
Special Investment Officer
Pension Investment and Cash Management
Office of the State Comptroller
59 Maiden Lane Fl. 30
New York, NY 10038
tgoldsmith@osc.state.ny.us
Direct Line: 212.383.2592
Receptionist: 212.383.3931
Facsimile: 212.383.1331

THOMAS P. DiNAPOLI
STATE COMPTROLLER

DIVISION OF CORPORATE GOVERNANCE
59 Maiden Lane-30th Floor
New York, NY 10038
Tel: (212) 383-3931
Fax: (212) 681-4468

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

November 15, 2017

Mr. Martin P. Akins
Senior Vice President, General Counsel
and Corporate Secretary
Express Scripts Holding Company
One Express Way
Saint Louis, Missouri 63121

Dear Mr. Akins:

The Comptroller of the State of New York, Thomas P. DiNapoli, is the trustee of the New York State Common Retirement Fund (the "Fund") and the administrative head of the New York State and Local Retirement System. The Comptroller has authorized me to inform of his intention to sponsor the enclosed shareholder proposal for consideration of stockholders at the next annual meeting.

I submit the enclosed proposal to you in accordance with rule 14a-8 of the Securities Exchange Act of 1934 and ask that it be included in your proxy statement.

A letter from J.P. Morgan Chase, the Fund's custodial bank verifying the Fund's ownership of Express Scripts Holding Company shares, continually for over one year, is enclosed. The Fund intends to continue to hold at least $2,000 worth of these securities through the date of the annual meeting.

We would be happy to discuss this initiative with you. Should the board of Express Scripts Holding Company decide to endorse its provisions as company policy, the Comptroller will ask that the proposal be withdrawn from consideration at the annual meeting. Please feel free to contact me at 212-383-1343 should you have any further questions on this matter.

Sincerely,

Gianna McCarthy
Director of Corporate Governance

Enclosures

Cyber Risk Report

Prior to becoming the Chairman of the SEC, Jay Clayton wrote, "cyber-threats are among the most urgent risk to America's economic and national security and the personal safety of its citizens." As recently as October 2017, the Co-Director of SEC Division of Enforcement identified cybersecurity disclosure as a priority and subject of potential enforcement "where there may be a cyber-related disclosure failure by a public company."

In 2017, the Healthcare Industry Cybersecurity Task Force noted the industry experienced more cyber incidents resulting in data breaches than any of the other 15 critical infrastructure sectors. According to a 2016 report by the Ponemon Institute, data breaches in healthcare are increasingly costly and frequent, and continue to put patient data at risk. The report estimates that data breaches could be costing the healthcare industry $6.2 billion.

In 2008, the Express Scripts Holding Company ("Company") disclosed a data breach affecting personal and medical information of over 700,000 customers.

The Company recognized in its 2017 10-K that:

[The Company's] ability to conduct operations depends on the security and stability of our technology infrastructure as well as the effectiveness of, and our ability to execute, business continuity plans across our operations. A failure in the security of our technology infrastructure or a significant disruption in service within our operations could materially adversely affect our business and results of operations.

However, the Company has not provided shareholders with a full report regarding this risk and its policies, procedures or other information concerning how it mitigates this risk.

RESOLVED: The Company's shareholders ask the Board to review and publicly report (at reasonable cost, in a reasonable timeframe, and omitting proprietary and confidential information) on its cyber risk and actions taken to mitigate that risk. A report adequate for investors to assess practices should include:

aspects of business or operations that give rise to material cyber risk;

the extent to which the Company outsources functions that have material cyber risks, descriptions of those functions and how the Company addresses those risks;

descriptions of cyber incidents experienced by the Company that individually or in the aggregate are material, including a description of costs and consequences;

risks related to cyber incidents that remain undetected for an extended period;

description of relevant insurance coverage;

compliance, regulatory or contractual obligations related to cyber risk;

certification to widely recognized standards; and

how cyber risks and cyber incidents are reflected in financial statements.

The report should also discuss the scope and frequency of the Board's oversight of cyber risks which may include review of relevant systems, policies, and procedures, related to:

- determining critical assets (e.g., customer information);
- employee training on data security and privacy-related risks;
- due diligence for third party vendors and potential acquisitions;
- data breach and incident response plans;
- minimization of data collection and retention; and
- security policies and audit frequency

J.P.Morgan

Miriam G. Awad
Vice President
CIB Client Service Americas

November 15, 2017

Mr. Martin P. Akins
Senior Vice President, General Counsel and Corporate Secretary
Express Scripts Holding Co.
One Express Way
Saint Louis, Missouri 63121

Dear Mr. Akins,

This letter is in response to a request by The Honorable Thomas P. DiNapoli, New York State Comptroller, regarding confirmation from JP Morgan Chase that the New York State Common Retirement Fund has been a beneficial owner of Express Scripts Holding Co. continuously for at least one year as of and including November 15, 2017.

Please note that J.P. Morgan Chase, as custodian for the New York State Common Retirement Fund, held a total of 1,581,380 shares of common stock as of November 15, 2017 and continues to hold shares in the company. The value of the ownership stake continuously held by the New York State Common Retirement Fund had a market value of at least $2,000.00 for at least twelve months prior to, and including, said date.

If there are any questions, please contact me at (212) 623-8481.

Regards,

Miriam Awad

cc: Gianna McCarthy- NYSCRF
Tana Goldsmith – NYSCRF
Kyle Seeley - NYSCRF

4 Chase Metrotech Center 6th Floor, Brooklyn, NY 11245
Telephone: +1 212 623 8481 Facsimile: +1 718 242 4506 miriam.g.awad@jpmorgan.com
JPMorgan Chase Bank, N.A.