GLOBAL BUSINESS TRAVEL ASSOCIATION

Business Travel Payment and Data Security:

Protecting Data & Mitigating Risk In The Digital Age

April 2019

Our Sponsor:

AirPlus INTERNATIONAL

Table of Contents

Introduction

Every year, data breaches expose billions of records worldwide.[1] [2] In most cases (76%), perpetrators are financially motivated.[3] For several reasons, corporate travel programs may be particularly vulnerable:

1) **Vendor data:** Travel involves financial transactions with a multitude of vendors including airlines, hotels, and retailers. In addition, managed programs rely on key service providers—such as TMCs—which may store personal or financial data for an extended period, and transmit data to other parties.

2) **Data security:** While traveling, employees may use unencrypted public Wi-Fi, commonly found in airports, hotels, and public spaces.

3) **Accommodations breaches:** Hospitality companies are particularly vulnerable to payment-related data breaches. The accommodations industry experienced 338 breaches over a recent one-year span, with a large majority (90%) of these targeting point-of-sale systems. [4]

This study examines data and payments security within managed corporate travel. It is based on a survey of U.S.-based travel managers, and focuses on two areas in particular:[5]

[1] Snider, Mike. "Your data was probably stolen in a cyberattack in 2018 – and you should care." *USA Today*, December 28, 2018. https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002/
[2] Graham, Luke. "The number of devastating cyberattacks is soaring – and it's likely to get much worse." *CNBC.com*, September 20, 2017. https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html
[3] Verizon Enterprise Solutions, *2018 Data Breach Investigations Report* (Verizon Wireless, 2018), 5.
[4] Ibid, 27.
[5] Note: The definitions below were also shown to survey respondents.

1) **External fraud:** Unauthorized use of company funds or payment data by an outsider such as a hacker or thief.

2) **Traveler misuse:** Out-of-policy spending by business travelers and employee cardholders.

While examining these topics, the study addresses several specific questions:

1) Do travel managers think fraud risk has increased, decreased, or remained constant in recent years?

2) How do travel programs respond when affected by a data breach?

3) Which security-related payment functions are travel programs typically involved with?

4) Which payment methods are most effective at preventing fraud? Which are most effective at preventing traveler misuse?

5) To what extent do travel programs apply payment controls to curb fraud or employee misuse? How do companies configure their expense management tools?

Methodology

An online survey was conducted of U.S. - based travel managers who are GBTA members. Data collection took place between January 16, 2019 and January 28, 2019.

An email invitation was sent to 1,187 GBTA buyer members in the U.S. Two hundred and eighteen recipients completed at least one question, for a response rate of 18%. Of these, 184 qualified because they were a travel manager/buyer

or procurement/sourcing professional, and have at least some involvement in "making decisions about payment solution providers and policies as they relate to travel." Of those who qualified, three-quarters (78%) completed the entire survey, for a total response of 144 travel managers.

Summary of Findings

The impact of fraud and data breaches

- **Travel managers think the risk of fraud is growing.** Two-thirds (68%) say travel programs face *greater risk* of fraud today than they did 2-3 years ago. Only 8% say they face *less risk* today.

- **Most travel managers (81%) are concerned about data breaches, with 37% being "very concerned."** Only one in eight (12%) are "not concerned" or "not concerned at all."

- **A large majority of travel programs have been impacted by a payment-related data breach in the past year.** More than two-thirds of Travel Managers (69%) say their business travelers have been affected by a breach of payment data from an outside vendor such as an airline, hotel, or retailer. Notably, one in five (22%) are "not sure," and only 9% are confident they have not been affected.

- **While other types of breaches occur, they are far less common.** One in eight travel programs (13%) has been affected by a breach of a corporate payment institution (e.g. a bank) in the past year.[6] Only 3% say

[6] In addition, 49% say their business travelers *have not* been affected by a payment-related data breach of a corporate payment institution, while 38% are not sure.

they have been affected by a breach of payment data from their own internal system(s).[7]

- **When impacted by a breach in the past year, six in 10 (58%) Travel Managers say their organization *alerted employees*, followed by *canceling and reissuing corporate cards* (44%), *monitoring corporate card statements* (37%), and *working with their payment provider* (28%).** Fewer *provided employees access to credit monitoring* (14%). [8] [9]

- **Companies learn about data breaches from a variety of sources.**[10] [11] Among those impacted in the past year, most travel managers (70%) say their organization was *notified by the vendor who suffered the breach*, and half (49%) heard about it from *news reports*. Alarmingly, far fewer were notified by their *payment provider* (31%), their *TMC* (27%), or their *travelers* (22%).

To what extent are travel programs involved with payment security?

- **About half of travel departments are involved with various payment security functions.** Most are involved with *responding to payment fraud by an external party* (58%), *educating travelers about payment security* (53%), and *setting policies related to payment security* (53%).[12] Some are

[7] In addition, 79% say their business travelers have not been affected by a payment-related data breach of their own internal system(s), while 18% are not sure.
[8] Note: The stats reported are based on a survey question asking respondents how their organization responded to *the last data breach* that affected their travelers.
[9] Note: The stats reported are based on a question that allowed multiple answers.
[10] Note: The stats reported are based on a question that allowed multiple answers.
[11] Note: The stats reported are based on a survey question asking respondents how their organization responded to *the last data breach* that affected their travelers.
[12] The statistics reported represent the share of respondents who indicated they are "involved" or "very involved" with these functions. The remainder indicated they were "not involved" or "not involved at all."

involved with *responding to lost or stolen corporate credit cards* (47%) and *evaluating the data security standards of payment suppliers* (43%). Surprisingly, involvement does not vary much by travel spend volume or travel program reach (i.e., national vs. global).

When travel departments are involved with payment security, they typically are collaborating with other departments – such as *finance/accounting/internal audit* (86%), *information technology* (62%), *legal/compliance* (58%) and *human resources* (48%).

- **Companies commonly provide data security advice to business travelers – but they may not proactively communicate it.** Most respondents (62%) say their organization provides data security tips to

Many companies provide data security tips to business travelers. Here are some tips that they can provide to travelers:

- **Educate Yourself About Public Wi-Fi:** Employees should be careful about unencryptyed Wi-Fi, commonly found in airports and hotels, or about accessing certain information from public networks. Employees should also be careful about websites that use the HTTP protocol, instead of the more secure HTTPS protocol. In addition, they should log-off from public networks when not using a connected device.

- **Use Virtual Private Networks (VPNs):** When possible, employees should use VPNs to access data through public Wi-Fi. These offer additional security through "tunneling" and encryption.

- **Maintain Device Security:** Travelers should make sure their devices are password-protected, their passwords are effective, and all anti-virus software and operating systems are up-to-date.

Recommendations adapted from the following sources:

Norton. "8 cybersecurity tips for business travelers." Accessed February 20, 2019. https://us.norton.com/internetsecurity-mobile-8-cyber-security-tips-for-business-travelers.html

Nield, David. "Simple Steps to Protect Yourself on Public Wi-Fi." Wired, August 5, 2018. Accessed February 20, 2019. https://www.wired.com/story/public-wifi-safety-tips/

Biersdorfer, J.D. "Tunneling Through the Internet on Vacation." *New York Times*, August 22, 2017. Accessed February 20, 2019. https://www.nytimes.com/2017/08/22/technology/personaltech/tunneling-though-the-internet-on-vacation.html

business travelers.[13] Eighty percent of high-spend travel programs provide these tips, compared to half of low-spend[14] and medium-spend[15] programs.[16] When companies do provide tips, they commonly communicate them through a *company portal/Intranet* (74%) or their *travel policy* (65%). Fewer communicate tips proactively, through an *email/newsletter* (49%) or a *seminar/class* (46%).

Fraud prevention: Payment methods[17]

- **Single-use virtual cards are viewed as most effective at preventing fraud.** Most Travel Managers (79%) say they are "effective" or "very effective" when "preventing fraud by an external party such as a hacker or a thief." Almost none (3%) say they are ineffective.

- **While two-thirds (67%) of Travel Managers say corporate cards are effective, one-fifth (19%) say they are "ineffective" or "very ineffective" at preventing external fraud.**

[13] 62% say their organization "provides training or information to business travelers on how to keep company and personal data secure on the road." Twenty-seven percent say it does not provide such advice, while 11% are not sure.
[14] 54% of low-spend programs provide such tips.
[15] 51% of medium-spend programs provide such tips.
[16] "Low-spend" programs are classified as those with annual travel spend of less than $10 million; "medium-spend" programs are those with spend of $10 million to less than $50 million; "high-spend" programs are those with spend of at least $50 million.
[17] Each stat reported below is among Travel Managers who indicated they had heard of the specified payment method.

- Few Travel Managers think *company cash advances* (33%), *pre-paid debit cards* (31%), or *employee personal funds* (19%) are effective at preventing external fraud.

Fraud prevention: Payment controls

- **Payment controls can prevent fraud and misuse.** Travel managers think different controls are valuable. These include *restricting certain merchant category types* (79%), *limiting the amount allowed in a single transaction* (64%), *restricting payment within a certain country or location* (55%), *setting daily or weekly spending limits* (49%).

- Nevertheless, many companies do apply these controls.

    - Most travel managers (61%) say their payment solutions are "never" or "rarely" configured to *restrict payment to a particular time period*. **Corporate credit cards typically do not offer this control.**

Virtual cards are on the rise, and are viewed as an effective weapon against fraud

- One-fifth of travel programs use single-use virtual card numbers, up from 11% last year*

- **Virtual cards have several features that might help prevent fraud and employee misuse, including:**

    - Each number expires after one-time use

    - They are typically used with strict payment controls, restricting payment to a specific merchant type, dollar amount, time period, or location

*20% of respondents to the current survey say their company uses single-use virtual card numbers.

*11% of respondents indicated they used virtual cards in a survey conducted last year. This can be found in the report *Five Business Travel Payment Trends*, published by GBTA,

- Most (60%) say their payment solutions are "never" or "rarely" configured to *restrict payment within a particular country or location*, despite half (55%) saying this control is valuable. Such controls can prevent fraud when card numbers are exposed in a data breach.

- Half (52%) "never" or "rarely" *set daily or weekly spending limit*s. Only one-third (31%) "always" or "often" apply this control.

- While four in 10 (41%) "always" or "often" *limit the amount allowed in a single transaction*, a similar number (38%) "never" or "rarely" do so.

- More than half (57%) say their payment solutions are "always" or "often" configured to *restrict certain merchant category types*. When

While Travel Managers think payment controls are valuable, many "never" or "rarely" use them. What explains this gap?

- **Difficulty of administration:** When payment controls are configured for corporate cards, companies can apply the same controls to all cards, or configure them individually or in "batches." This process can be time-consuming. In addition, companies only have limited flexibility to apply different controls to different travelers

- **Prevents legitimate use:** Payment controls can prevent travelers from making legitimate purchases. For example, travelers may be unable to make purchases abroad when their credit card restricts payment to a particular country. This is especially the case when corporate cards are the only authorized payment method

- **Goes against company culture:** Payment controls may not always fit company culture. Increasingly, companies trust employees to do the right thing. However, as the risk of fraud grows, payment controls may be needed to combat *external fraud*, even when they are not needed to prevent employee misuse

companies apply this control, they typically configure **corporate cards** to restrict spending at merchants such as retail stores and night clubs. Yet it can be difficult to "tailor" this control to specific situations. However, this may change as more companies adopt single-use virtual cards, which are commonly used to restrict spending to a single merchant, such as a hotel, or restrict specific amenities or upgrades.

Business traveler misuse: Payment methods[18]

- **When it comes to preventing business traveler *misuse*, Travel Managers feel Central Travel Accounts (CTAs) are the most effective payment method.** CTAs are also known as "lodge" or "ghost" accounts, and are typically stored with a TMC or in a booking tool, thus preventing travelers from making out-of-policy decisions.

- **A majority (72%) of Travel Managers think *corporate cards* are effective at preventing traveler misuse.** This may come as a surprise given fairly limited use of payment controls (see previous page), and 15% say corporate cards are "ineffective" or "very ineffective."

Are Travel Managers concerned about employee misuse?

- **63%** are concerned about employee spending on out-of-policy upgrades such as business class or hotel suites
- **56%** are concerned about employee spending on out-of-policy items such as merchandise or alcohol
- **36%** are concerned about employees exceeding per diems

Numbers reported are the percentage who are "concerned" or "very concerned"

[18] Each statistic reported below is only from among the group of Travel Managers who indicated they had heard of the specified payment method.

Single-use virtual card numbers are perceived as being effective at preventing traveler misuse, with seven in 10 (70%) saying they are effective, and only 4% saying they are ineffective. One-quarter (26%) have "no opinion," reflecting limited knowledge about single-use cards.

- **Several methods are rarely viewed as effective.** These include *company cash advances* (26%), *pre-paid debit cards* (26%), and *employee personal funds* (22%).

Preventing misuse: Expense tool configuration

- **In many cases, companies identify fraud or misuse during the expense process.** The box at right shows how companies configure their expense tool to identify potential cases of fraud or misuse.

Do companies configure their expense tool to flag or "mark exceptions" for…?

- **75%** expense reports with missing information or documentation (e.g. receipts or form fields)
- **66%** out-of-policy expenses
- **47%** expense types above a certain amount (e.g. air, hotel, or dinner)
- **40%** transactions with certain types of merchants (e.g. retail stores or nightclubs)
- **36%** expense reports above a certain overall amount
- **23%** expense reports that are filed by travelers who have submitted problematic expense reports in the past

Conclusion

Most Travel Managers think the risk of fraud is growing. Travel programs should consider several steps to protect against fraud and misuse:

1) **Communicate proactively:** While most travel programs (62%) provide data security tips, they commonly communicate them through a

passive method such as their travel policy, and rarely update them. Companies should consider communicating these tips more proactively and more often – via email or newsletter or their booking tool.

2) **Advocate and translate for travelers:** About half of travel programs are involved with payment security functions of some type, such as *responding to payment fraud by an external party* (58%), or *educating travelers about payment security* (53%). Even they are not involved, they can still play a role. They can serve as a "bridge" between travelers and other departments. For instance, they can relay traveler feedback about payment security policies to relevant departments – such as finance/accounting. In the other direction, they can explain the payment security policies to travelers.

3) **Consider payment controls:** Even though most Travel Managers think payment controls are valuable, a notable share "never" or "rarely" use them. These travel programs might consider applying controls more. Companies might benefit from restricting certain types of merchants and from restricting payment within a particular country or countries– two controls that are especially effective in preventing external fraud.

Works Cited

Biersdorfer, J.D. “Tunneling Through the Internet on Vacation.” *New York Times*, August 22, 2017. Accessed February 20, 2019. https://www.nytimes.com/2017/08/22/technology/personaltech/tunneling-though-the-internet-on-vacation.html.

GBTA, *Five Business Travel Payment Trends: Summary of Findings*. Alexandria, VA: GBTA, 2018.

Graham, Luke. “The number of devastating cyberattacks is soaring – and it’s likely to get much worse.” *CNBC.com*, September 20, 2017. https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html.

Nield, David. “Simple Steps to Protect Yourself on Public Wi-Fi.” Wired, August 5, 2018. Accessed February 20, 2019. https://www.wired.com/story/public-wifi-safety-tips/.

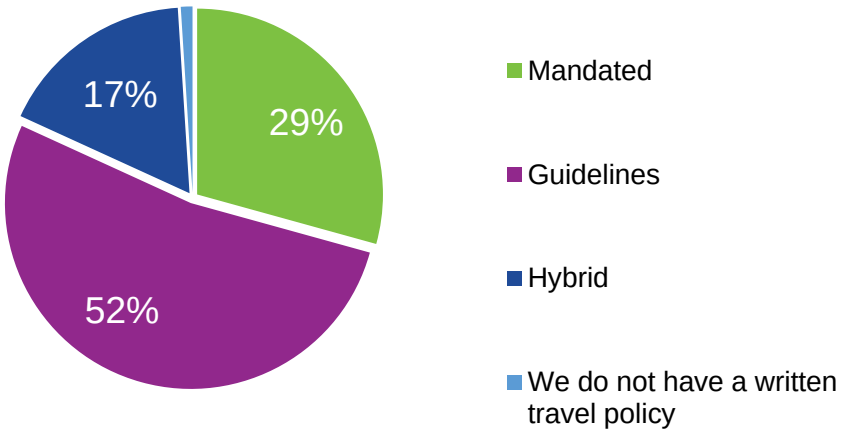
Norton. “8 cybersecurity tips for business travelers.” Accessed February 20, 2019. https://us.norton.com/internetsecurity-mobile-8-cyber-security-tips-for-business-travelers.html

Snider, Mike. “Your data was probably stolen in a cyberattack in 2018 – and you should care.” *USA Today*, December 28, 2018. https://www.usatoday.com/story/money/2018/12/28/data-breaches-2018-billions-hit-growing-number-cyberattacks/2413411002/.

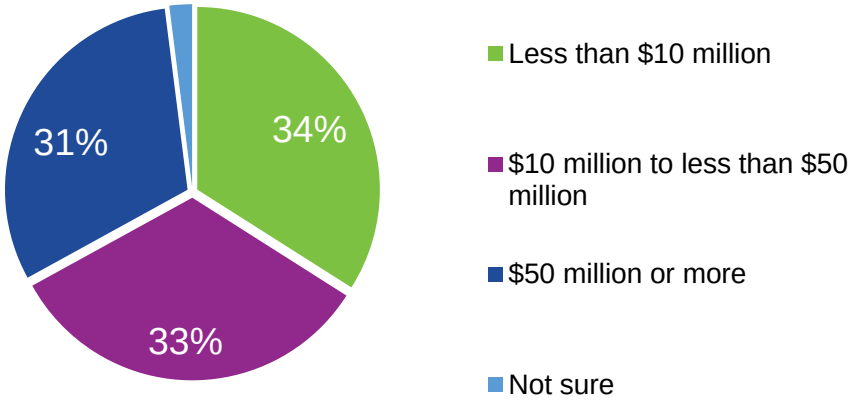
Verizon Enterprise Solutions, *2018 Data Breach Investigations Report*. Verizon Wireless, 2018.

Respondent Profile

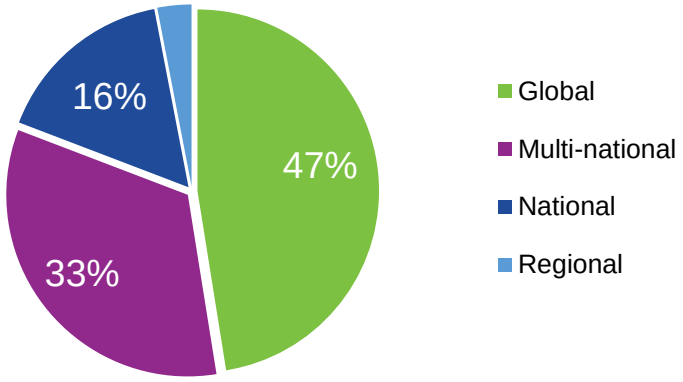
In general, which statement best describes your organization's travel policy? (n=144)



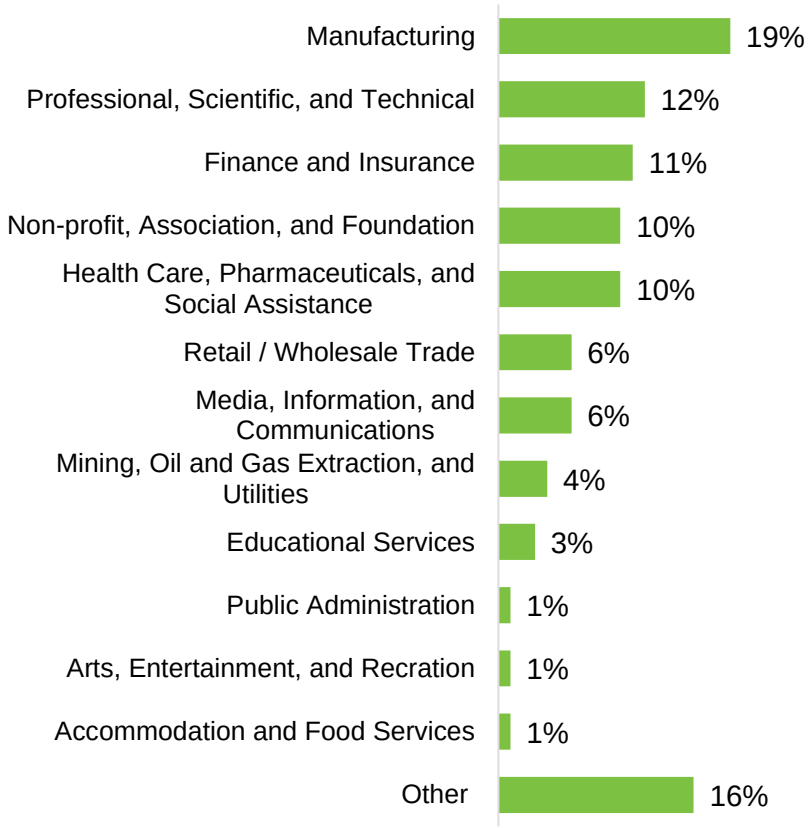
What was your total travel spend in 2018 in U.S. dollars (including air, hotel, car rentals, meetings, etc.)?
Please use your best estimate. (n=143)



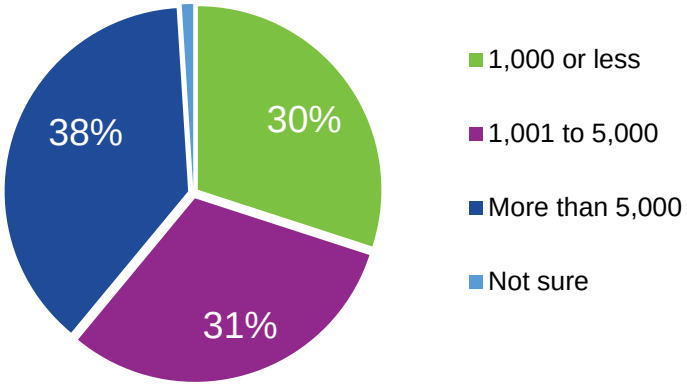
How would you define your company's reach? (n=144)



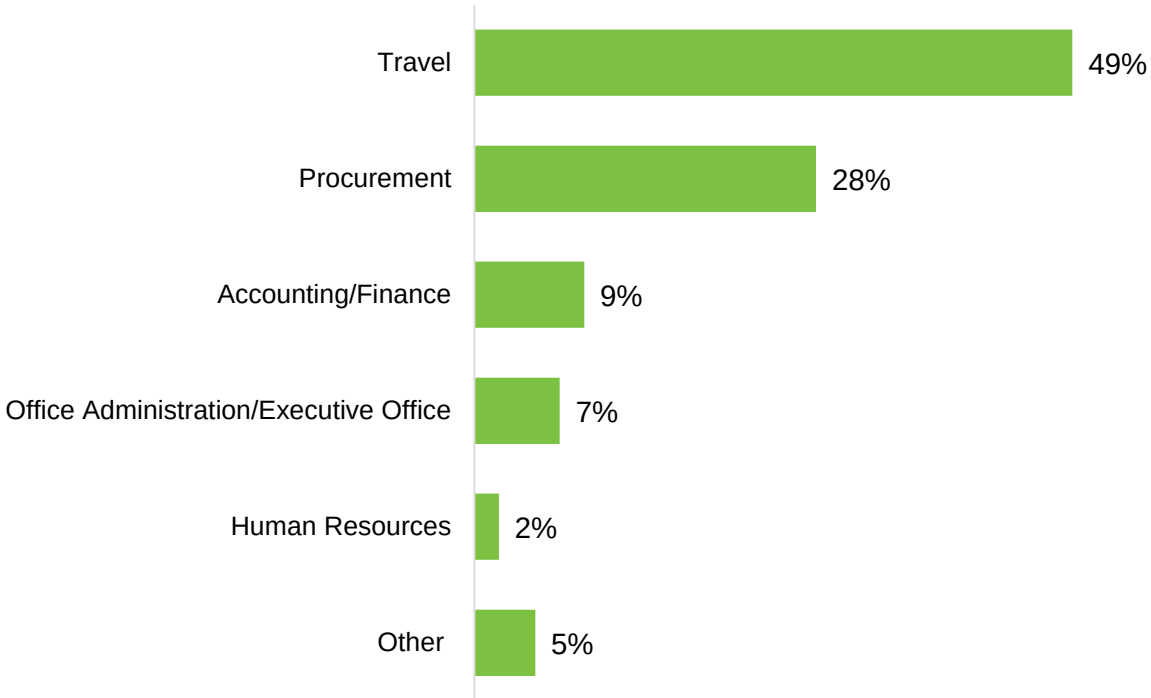
Which of the following industries best describes your organization? (n=144)



In 2018, approximately how many employees traveled on behalf of your company?
Your best estimate is fine. (n=144)



Which of these areas most closely resembles the department in which you work? (n=144)



About GBTA

The Global Business Travel Association (GBTA) is the world's premier business travel and meetings trade organization headquartered in the Washington, D.C. area with operations on six continents. GBTA's 9,000-plus members manage more than $345 billion of global business travel and meetings expenditures annually. GBTA delivers world-class education, events, research, advocacy and media to a growing global network of more than 28,000 travel professionals and 125,000 active contacts. To learn how business travel drives lasting business growth, visit gbta.org.

About AirPlus

AirPlus is a leading international provider of payment solutions for the day-to-day management of business travel. More than 51,000 corporate clients in 60 countries count on AirPlus for the payment and analysis of their business trip costs. Products and services such as central bill accounts, single-use virtual cards, corporate cards and online management tools are marketed worldwide under the AirPlus International brand. AirPlus, the leading issuer of UATP worldwide, is travel agency neutral. For more information, please visit www.airplus.com.