SpyCloud

2020 Report:
Breach Exposure of the Fortune 1000

SpyCloud

2020 Report: **Breach Exposure of the Fortune 1000**

Overview

It's human nature: people reuse passwords. Unfortunately, those reused passwords can easily become exposed to cybercriminals and used for malicious intent. According to the 2019 Verizon Data Breach Report, the use of weak and stolen credentials ranked as the most common hacking tactic for the third year in a row.

Password reuse represents a particularly significant security risk for enterprises, which house valuable corporate secrets and represent lucrative targets for cybercriminals. Employees frequently reuse corporate credentials as personal logins, regardless of security guidelines that prohibit such behavior. When those third-party sites are subject to data breaches, reused employee logins provide easy entry points to corporate systems and networks.

In addition to corporate credentials, data breaches expose a wealth of personal information that can enable cybercriminals to bypass security measures, take over accounts, and compromise enterprise networks. Employees, trusted partners, and suppliers with privileged access can all be vulnerable to account takeover and business email compromise.

With nearly 100 billion recovered breach assets collected to date, SpyCloud maintains the world's largest repository of recovered stolen credentials and PII. SpyCloud researchers continually monitor the criminal underground for breach data that has become available to cybercriminals, using human intelligence to gain access to stolen data as soon as possible after a breach occurs.

To provide a snapshot of the breach exposure affecting major enterprises, we examined SpyCloud's entire database to see what breach data we could tie to companies in the Fortune 1000. To do so, we searched for breach records containing Fortune 1000 corporate email domains, excluding "freemail" domains that are available to consumers. For example, if a Fortune 1000 employee signed up for a breached third-party site using their corporate email address, example@employer.com, we were able to tie the resulting breach record to their employer.

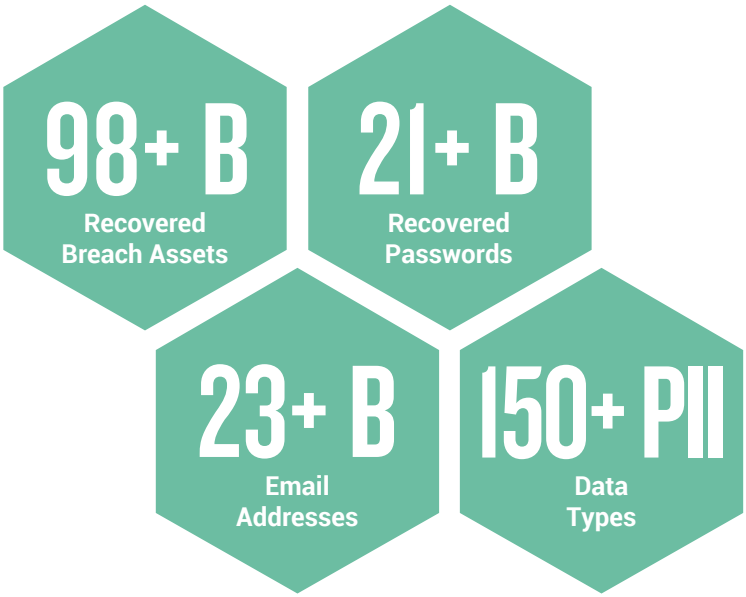
We were able to identify over 412 million breach assets within our dataset tied to employees in the Fortune 1000. Within this analysis, we have broken that number down by data type and sector (as defined by ***Fortune***) to reveal the scope of the breach exposure facing different sectors.

Bear in mind that corporate employees also have personal aliases that aren't reflected in this analysis, which can also be tied to corporate identities and used for illicit gain. In addition, this data will capture some employees who have moved on to other companies. However, we hope that this analysis provides a window into the scale of the account takeover risks facing large enterprises and the importance of monitoring employee credentials for weak and reused passwords.

About SpyCloud Data

Current, Relevant, Truly Actionable

SpyCloud uses Human Intelligence (HUMINT) to quickly recover current breach data within days of the breach occurring. Our unique data cleansing and password decryption process reveals exposed credentials faster and with greater match rates. Not only is our breach database the cleanest, we provide the most data of any provider, with context and perspective to make it immediately actionable. **Learn more at spycloud.com**.



Key Findings

1. Employees of the Fortune 1000 are just as bad about reusing passwords as the rest of us.

We found password reuse at a rate of 76.5 percent across the breached corporate credentials in our dataset, including exact matches and slight variations.

2. The Telecommunications sector is the worst offender by far.

Employees in this sector have the highest average numbers of exposed PII assets, phone assets, geolocation assets, and plaintext corporate credentials per company.

3. Technology comes in second place – and has the highest numbers of potentially infected employees.

We recovered credentials from 1,022 Technology sector employees whose corporate or personal systems appear to be infected with keylogging malware.

4. The credentials of 127,083 C-level Fortune 1000 executives are available on the criminal underground.

On average, companies in the Hotels, Restaurants & Leisure sector have the most exposed C-level executives.

5. Credentials are only part of the story.

Beyond exposed passwords and potentially compromised users, bad actors have access to a wealth of compromised PII that can be used in targeted attacks – over 200M PII assets tied to Fortune 1000 employees are available to cybercriminals.

6. The most common passwords for the Media industry are mostly unprintable.

But for Fortune 1000 employees with family-friendly passwords, popular themes include first names, company names, and simple strings of numbers and letters (123456, abc123, password).

At a Glance: Breach Exposure of the Fortune 1000

32,468

TOTAL BREACH SOURCES

Total number of breaches in the SpyCloud dataset that include records tied to Fortune 1000 corporate email addresses.

76,113,878

TOTAL CORPORATE BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. Ex: Information tied to jsmith@acme.com within a set of data stolen in a breach of example.com.

412,761,443

TOTAL BREACH ASSETS

A breach asset is a piece of information contained within a breach record. Ex: a password, an address, a phone number.

23,100,146

TOTAL PLAINTEXT CORPORATE CREDENTIALS

Total number of Fortune 1000 corporate email addresses and plaintext password pairs that have appeared in a data breach and are available to criminals. If employees have reused these passwords, criminals can easily exploit the exposed credential pairs to gain access to corporate systems.

127,083

TOTAL C-LEVEL EXECUTIVES EXPOSED

Exposed corporate credentials that are tied to Fortune 1000 executives with high-ranking titles, putting them at increased risk of targeted account takeover attempts and business email compromise (BEC) fraud.

76.5%

PASSWORD REUSE INDEX

Among the Fortune 1000 employees who appear in more than one breach, this is the rate of password reuse we have observed. This includes exact passwords and slight variations that criminals can easily match.

2,759

POTENTIALLY INFECTED EMPLOYEES

SpyCloud recovers some data collected by botnets. Credentials appearing in this data indicate that affected employees have malware with a keylogging component installed on their personal or corporate systems.

Corporate Credential Exposure of the Fortune 1000

Exposed Corporate Credentials by Sector

Across the SpyCloud dataset, we discovered 23 million pairs of credentials with Fortune 1000 corporate email addresses and plaintext passwords. While not every credential pair will match corporate login details, the ones that do match represent substantial risk for these enterprises—and their customers and partners.

When credentials are exposed in a data breach, cybercriminals inevitably test them against a variety of other online sites, taking over any other accounts protected by the same login information. If those stolen credentials contain a corporate email domain, criminals have an obvious clue that they could provide access to valuable enterprise systems, customer data, and intellectual property.

In theory, corporate passwords should be strong given the importance of the assets they protect and the robust guidance often provided by corporate security teams. In practice, many employees practice bad password hygiene at work, and some corporate password policies even encourage bad habits. Outdated policies like strict complexity rules and mandatory 90-day password rotations make passwords harder to remember, leading employees to make insecure choices like recycling versions of their favorite passwords. That's why the latest guidance from the National Institute of Standards and Technology (NIST) calls for organizations to proactively check for "commonly-used, expected, or compromised" user passwords to effectively mitigate the risk posed by human behavior.

In the SpyCloud database, we found:

Fortune 1000 Sector	Number of Companies	Total Exposed Corporate Credentials	Average Corporate Credentials per Company
Aerospace & Defense	23	401,890	17,473
Apparel	14	126,537	9,038
Business Services	50	426,492	8,530
Chemicals	30	234,846	7,828
Energy	118	694,026	5,882
Engineering & Construction	31	223,146	7,198
Financials	149	2,921,606	19,608
Food & Drug Stores	11	67,780	6,162
Food, Beverages & Tobacco	36	198,172	5,505
Healthcare	72	1,228,723	17,066
Hotels, Restaurants & Leisure	27	284,339	10,531
Household Products	27	332,622	12,319
Industrials	49	960,744	19,607
Materials	47	188,501	4,011
Media	26	1,205,368	46,360
Motor Vehicles & Parts	23	329,456	14,324
Retailing	73	825,720	11,311
Technology	105	6,180,690	58,864
Telecommunications	11	5,533,797	503,072
Transportation	40	508,820	12,721
Wholesalers	38	226,908	5,971
Total	**1000**	**23,100,183**	**23,100**

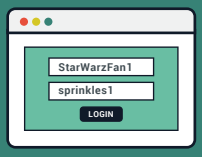
Password Reuse: Worst Offenders by Sector

Password reuse is rampant. In fact, 59 percent of people admit to using the same password everywhere. That trend holds true even for employees of the Fortune 1000, where you can imagine the stakes (and security measures) are especially high.

Within our dataset of Fortune 1000 corporate breach exposures, we examined how many employees with more than one exposed login have reused the same password or a close variation across multiple sites, then assigned a Password Reuse Index to each industry. The higher the percentage, the greater the rate of employee password reuse.

Employees with multiple reused passwords in our dataset may or may not reuse passwords at work—we can't tell for sure without checking their actual work passwords. However, password reuse across personal accounts does provide an indication of employees' overall password hygiene.

TOP 100 REUSED PASSWORDS



123456 password 123456789 nopassword password1 [company name] abc123 [redacted]off [company name] 12345678 111111 sunshine 12345 welcome 1234 [company name] qwerty maggie princess 1234567 bailey summer [company name] michael[redacted]cd [redacted]dork [company name]1 [redacted]cc baseball [redacted]ce [redacted]cb welcome1 charlie passport jordan ashley madison football 123456a [company name]5 soccer monkey taylor harley hunter passw0rd hannah matthew shadow buster 010203Zaq michael1 tigger 123123 jordan23 1234567890 peanut michelle aaaaaa andrew purple letmein ginger joshua jennifer 123abc justin party jesus1 jackson pepper jessica nicole lauren morgan mickey 123 mustang Password1 austin family zaq12wsx nicholas 1qaz2wsx amanda iloveyou samantha daniel yankees a123456 vacation princess1 sydney hockey

In the SpyCloud database, we found:

Rank	Sector	Password Reuse Index
1	Media	85%
2	Household Products	82%
3	Healthcare	80%
4	Hotels, Restaurants & Leisure	80%
5	Motor Vehicles & Parts	80%
6	Aerospace & Defense	79%
7	Engineering & Construction	79%
8	Business Services	78%
9	Transportation	78%
10	Technology	78%
11	Financials	77%
12	Materials	77%
13	Industrials	77%
14	Chemicals	77%
15	Food & Drug Stores	76%
16	Energy	76%
17	Telecommunications	74%
18	Apparel	74%
19	Food, Beverages & Tobacco	74%
20	Wholesalers	74%
21	Retailing	53%

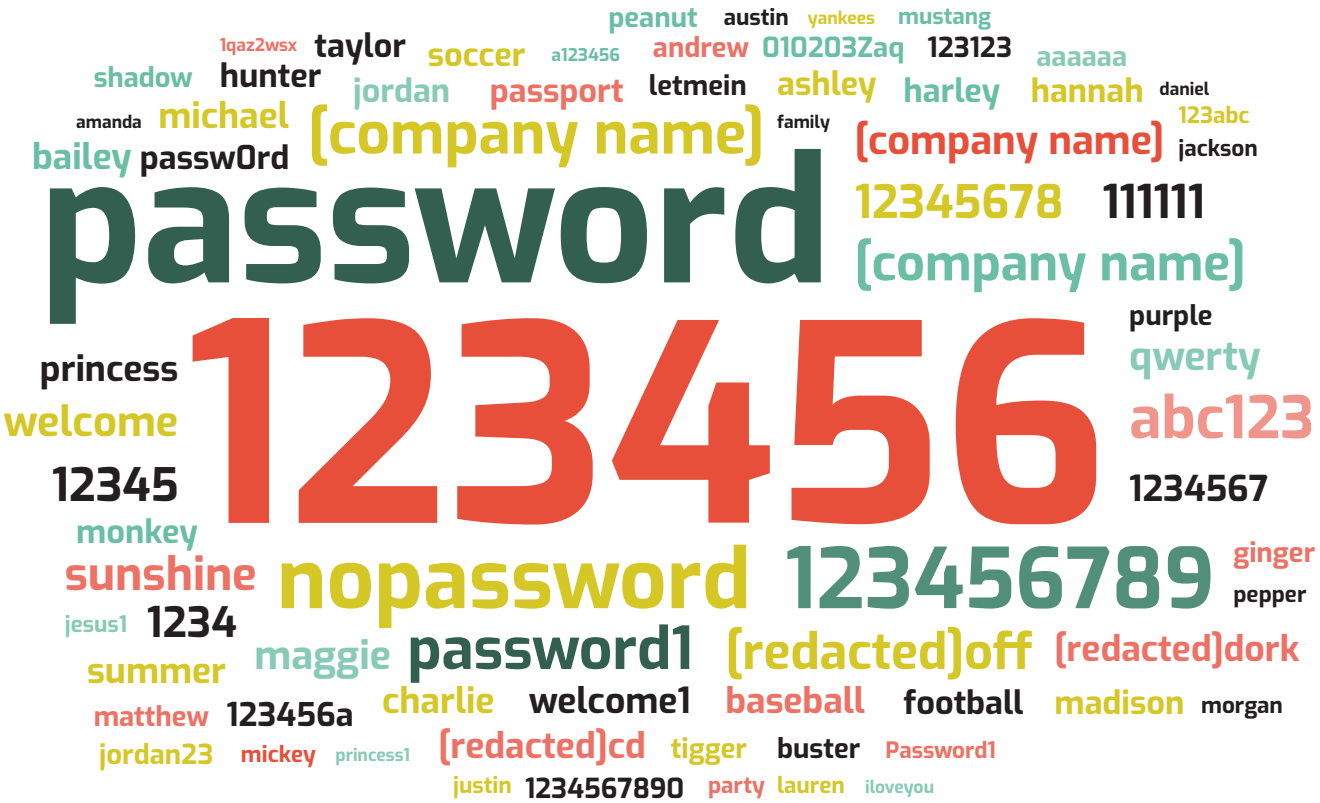
Favorite Passwords of Fortune 1000 Employees

With hundreds of accounts to keep track of, it's no wonder people take shortcuts to remember their login credentials. In addition to recycling variations of a few favorites across every account, people often use simple passwords that are easy to remember—and easy for criminals to guess. Criminals often use lists of common passwords in password spraying attacks, putting accounts with weak passwords at risk even if the user hasn't intentionally reused that password.

Fortune 1000 employees follow the same patterns as the rest of us. Each of the passwords below appeared hundreds or even thousands of times within our dataset. (We've redacted company names, which appeared very frequently, as well as several variations of a popular four-letter word that we opted not to print.)

While most of these examples would fail to pass basic corporate password policies, people tend to transform a base password in predictable ways to bypass complexity rules. For example, 'password' might become 'Password1' or 'Passw0rd!' at work. Unfortunately, criminals are well-aware of these patterns, and sophisticated account checker tools make it easy for criminals to test variations of exposed passwords at scale.

Popular Passwords of Fortune 1000 Employees



THE PASSWORD

123456

APPEARED 14,252 TIMES

THE PASSWORD

password

APPEARED 7,589 TIMES

THE PASSWORD

123456789

APPEARED 3,407 TIMES

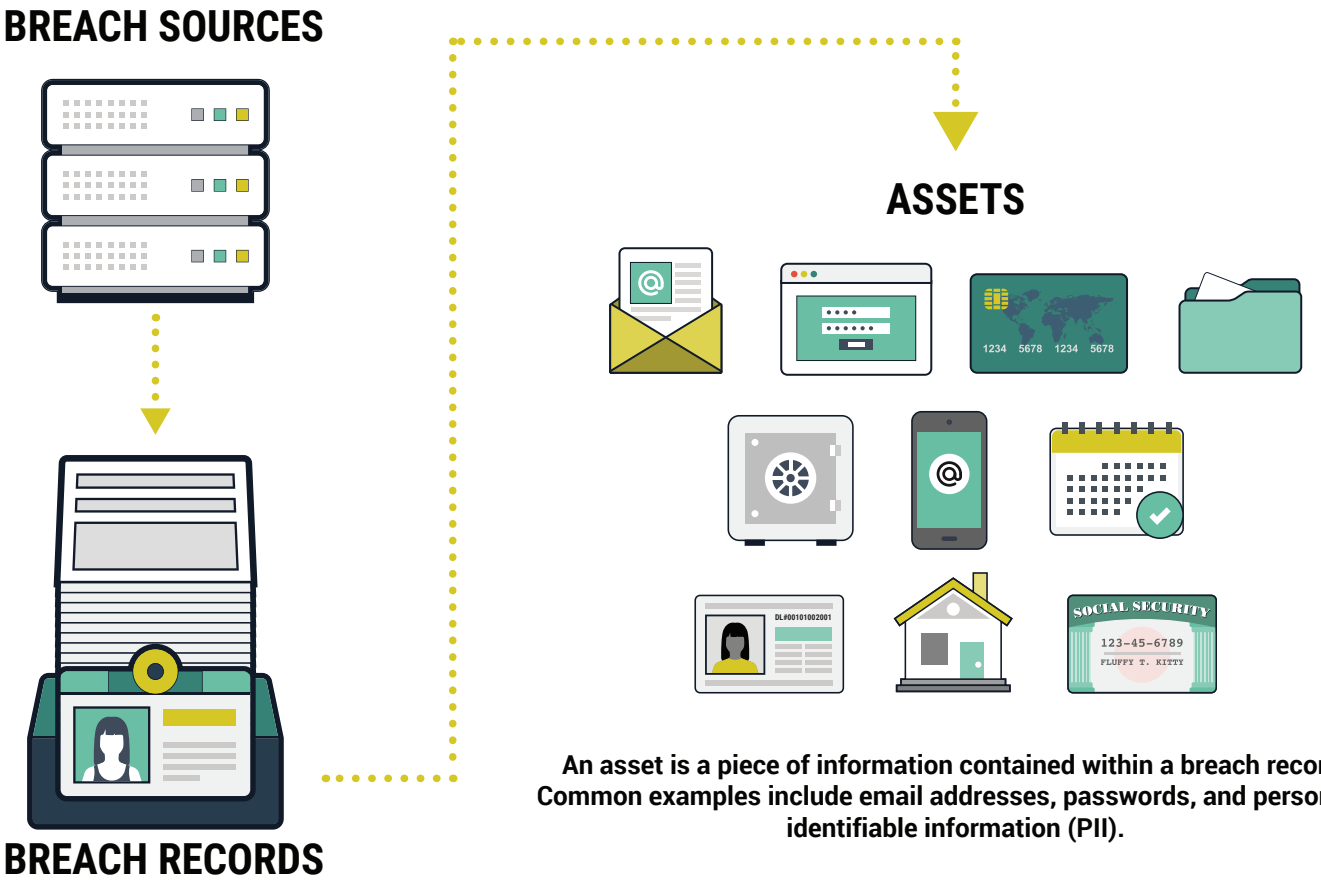
Beyond Credentials: Other Breach Exposures by Asset Type

A breach asset is a piece of information connected to a single breach record. In addition to login credentials, breach assets can include phone numbers, addresses, social security numbers, credit ratings, and much more—any type of information that can be obtained in a data breach. While stolen credentials provide an obvious entrypoint for malicious actors, other types of breach assets can also provide tremendous value to cybercriminals, whether for consumer fraud or as a means of gaining access to enterprise networks, data, intellectual property, and funds.

Criminals may engage in highly-targeted, manual attacks against victims with privileged access to corporate resources, such as C-suite leaders, senior executives, system administrators, and developers. Given the potential payoff associated with these targets, it's no wonder criminals are willing to invest substantial effort and creativity to take over their accounts. One criminal SpyCloud helped bring to justice tormented a leader at a nationally-recognized technology solutions firm for three years, stealing his identity and committing extensive financial fraud using his information.

In total, SpyCloud has collected 412,761,443 breach assets tied to Fortune 1000 employees.

Within the SpyCloud dataset, we have segmented certain types of breach assets into categories to help quantify different types of breach exposure. Let's break down how a few of these asset types can be used by cybercriminals and look at Fortune 1000 employee exposure for each asset type by sector.



An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Asset Type: Personally Identifiable Information (PII)

What It Is

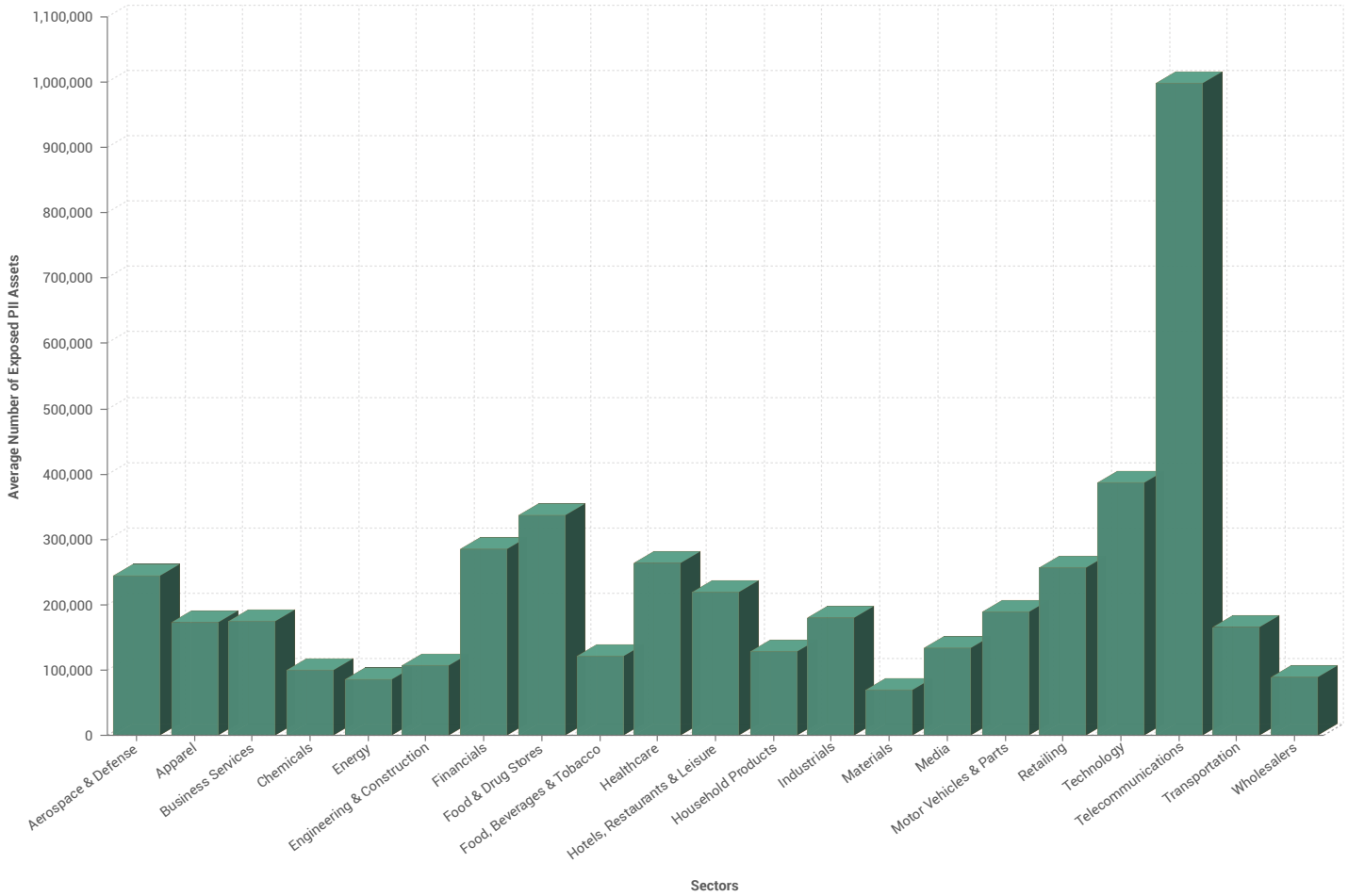
Personally identifiable information (PII) is data that could be used to identify an individual person. For the purposes of this report, SpyCloud has excluded some forms of PII that have been broken out into separate categories below, such as phone and financial assets. However, this category includes many other types of personal data such as addresses, social security information, and credit ratings.

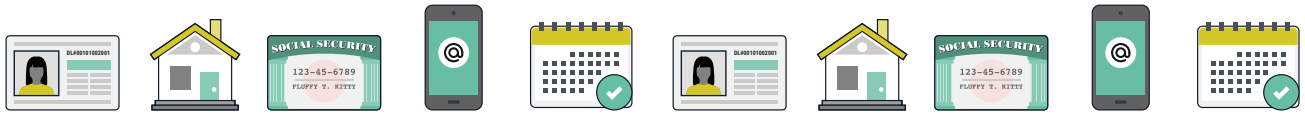
How It Helps Criminals

Personally identifiable information can provide criminals with many lucrative paths for committing fraud or stealing corporate data, particularly when they have access to full packages of victims' information, or "fullz." Using stolen PII, criminals can:

- **Steal a victim's identity to commit fraud, such as opening loans in their name**
- **Create new accounts to use as synthetic identities**
- **Craft detailed, credible spear phishing messages**
- **Submit fraudulent applications**

Exposures by Sector: Average Number of Exposed PII Assets per Company





Asset Type: Phone Assets

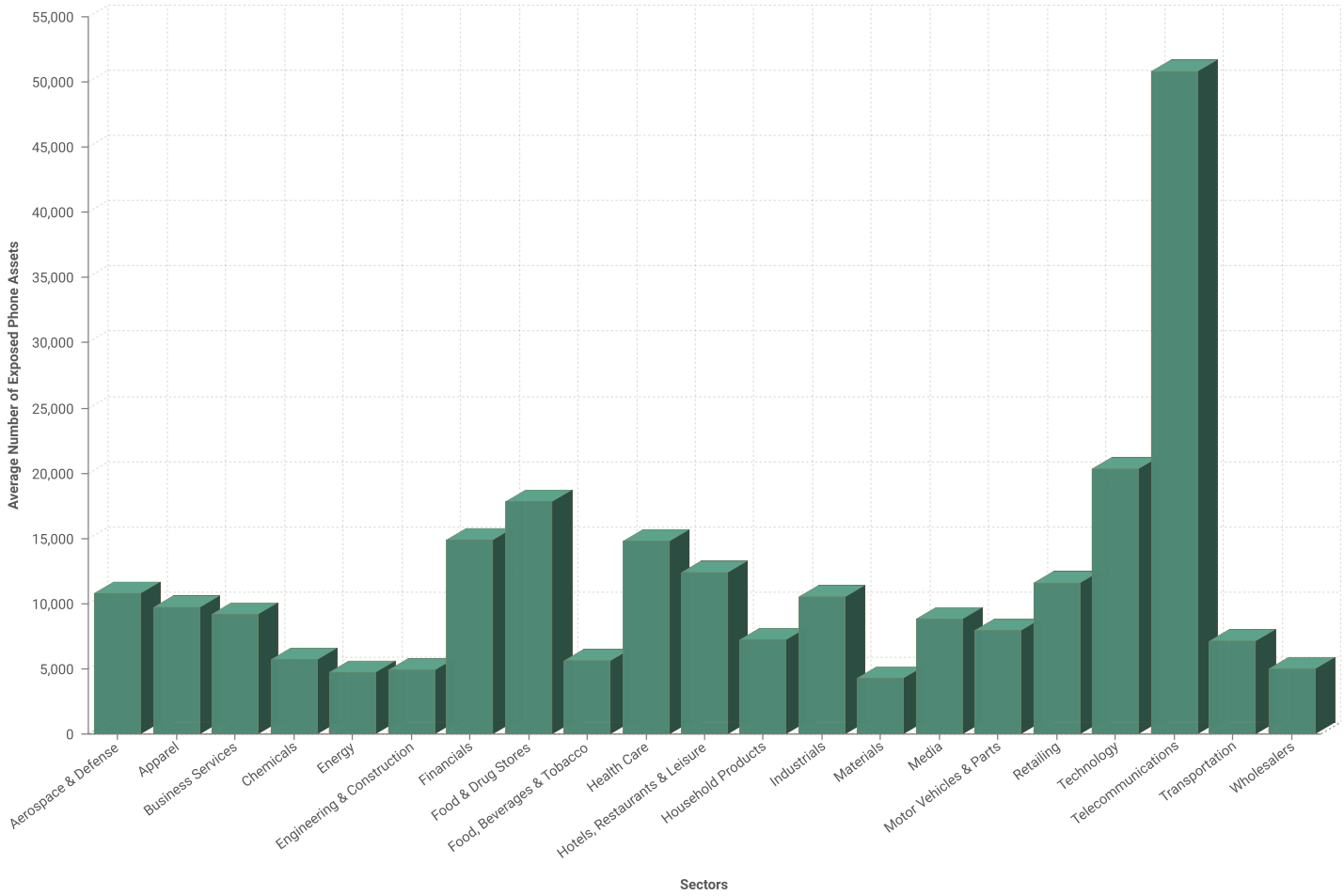
What It Is

Phone assets are stolen phone numbers.

How It Helps Criminals

In combination with stolen credentials, criminals can use phone assets to bypass multi-factor authentication using tactics such as SIM swapping and phone porting. With a simple phone call to a mobile carrier and some light social engineering, criminals can divert a victim's phone service to their own device. Once the attacker has control of the victim's phone number, they receive all SMS-based authentication messages and can easily log into sensitive accounts (even corporate accounts) undetected.

Exposures by Sector: Average Number of Exposed Phone Assets per Company



Asset Type: Geolocation

What It Is

Geolocation assets consist of latitude and longitude pairings that pinpoint users' physical locations. This is typically the location of the IP that a user last logged in from. That location sometimes correlates with their address, but not always, which is why this data has been separated from PII assets.

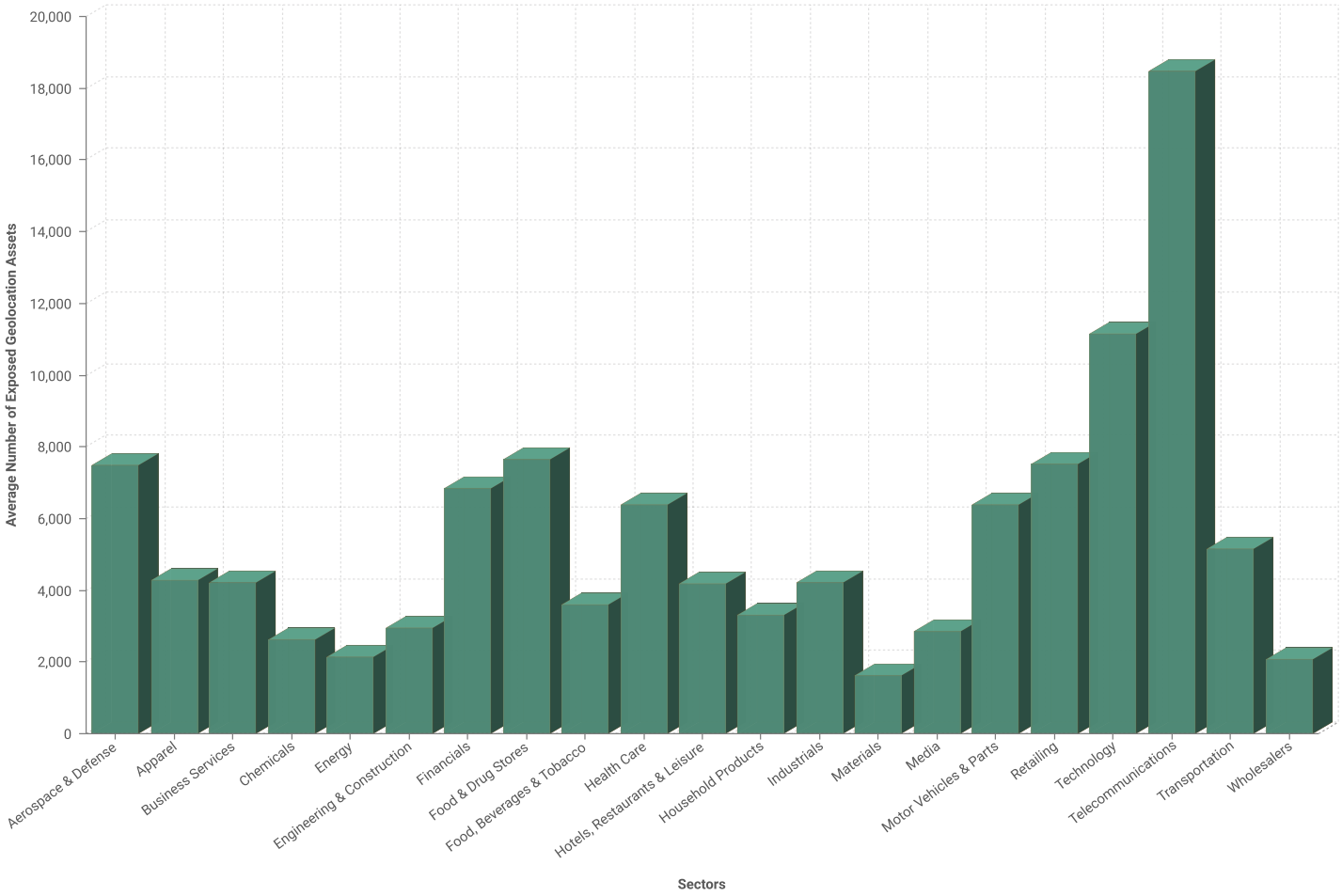
How It Helps Criminals

Criminals can use geolocation data (or addresses) to craft targeted attacks against high-value victims such as employees with privileged access to corporate data.

Examples include:

- **Using a VPN to mimic traffic from a user's location, avoiding controls that flag logins from unexpected locations**
- **Crafting spear phishing emails that reference the user's location, such as an event invitation that contains a malicious link**
- **Guessing the answers to knowledge-based security questions**

Exposures by Sector: Average Number of Exposed Geolocation Assets per Company



Asset Type: Financial

What It Is

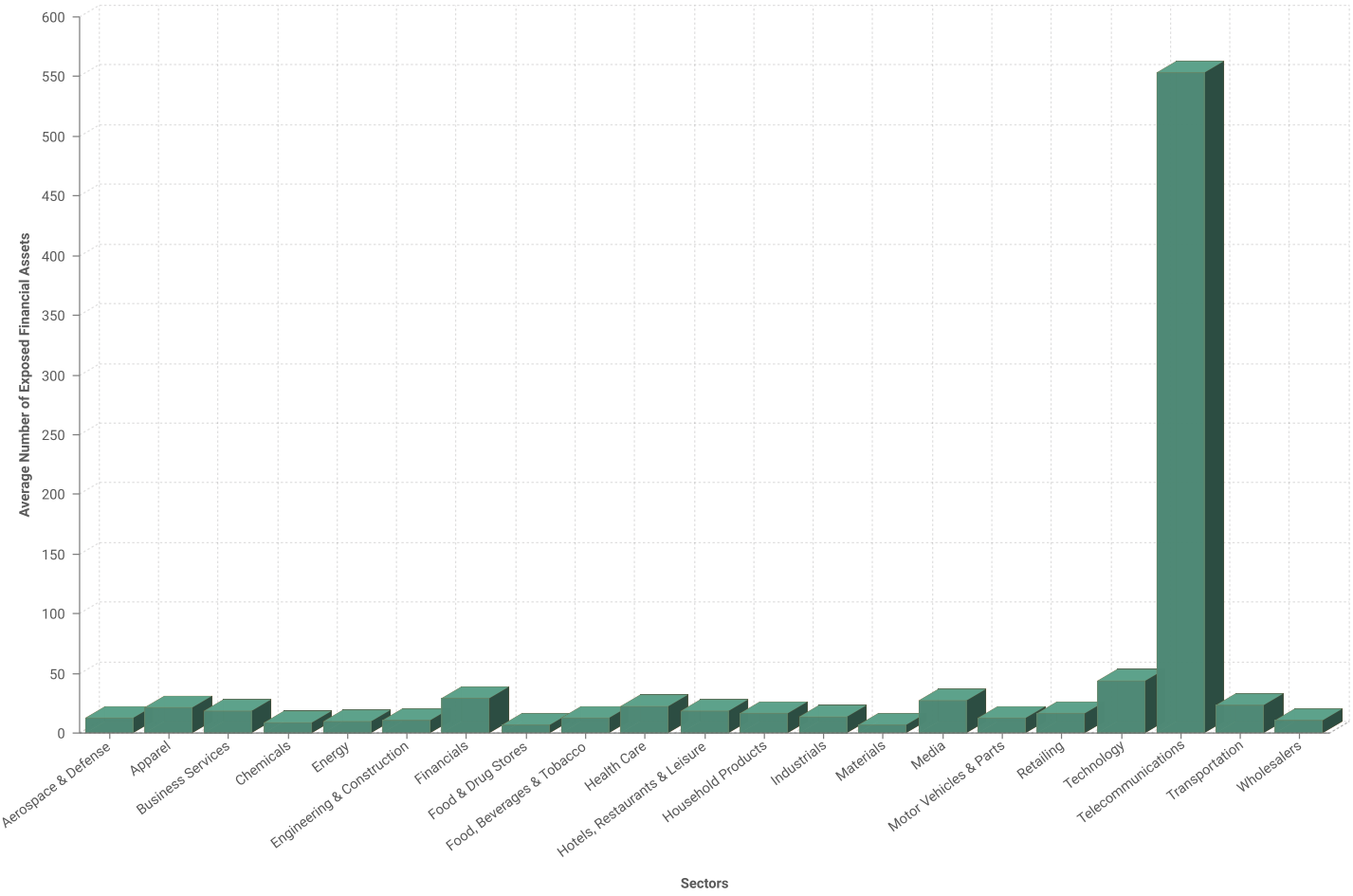
Financial assets include credit card numbers, bank account numbers, and tax IDs. While this information all technically qualifies as PII, we have separated them into their own category due to the severity of the exposure.

How It Helps Criminals

Criminals can use stolen credit card numbers and other financial information to:

- **Make fraudulent purchases**
- **Drain funds from accounts**
- **Resell card numbers and other stolen data to other criminals**
- **Collect victims' tax refunds**
- **Guessing the answers to knowledge-based security questions**

Exposures by Sector: Average Number of Exposed Financial Assets per Company



Asset Type: Social

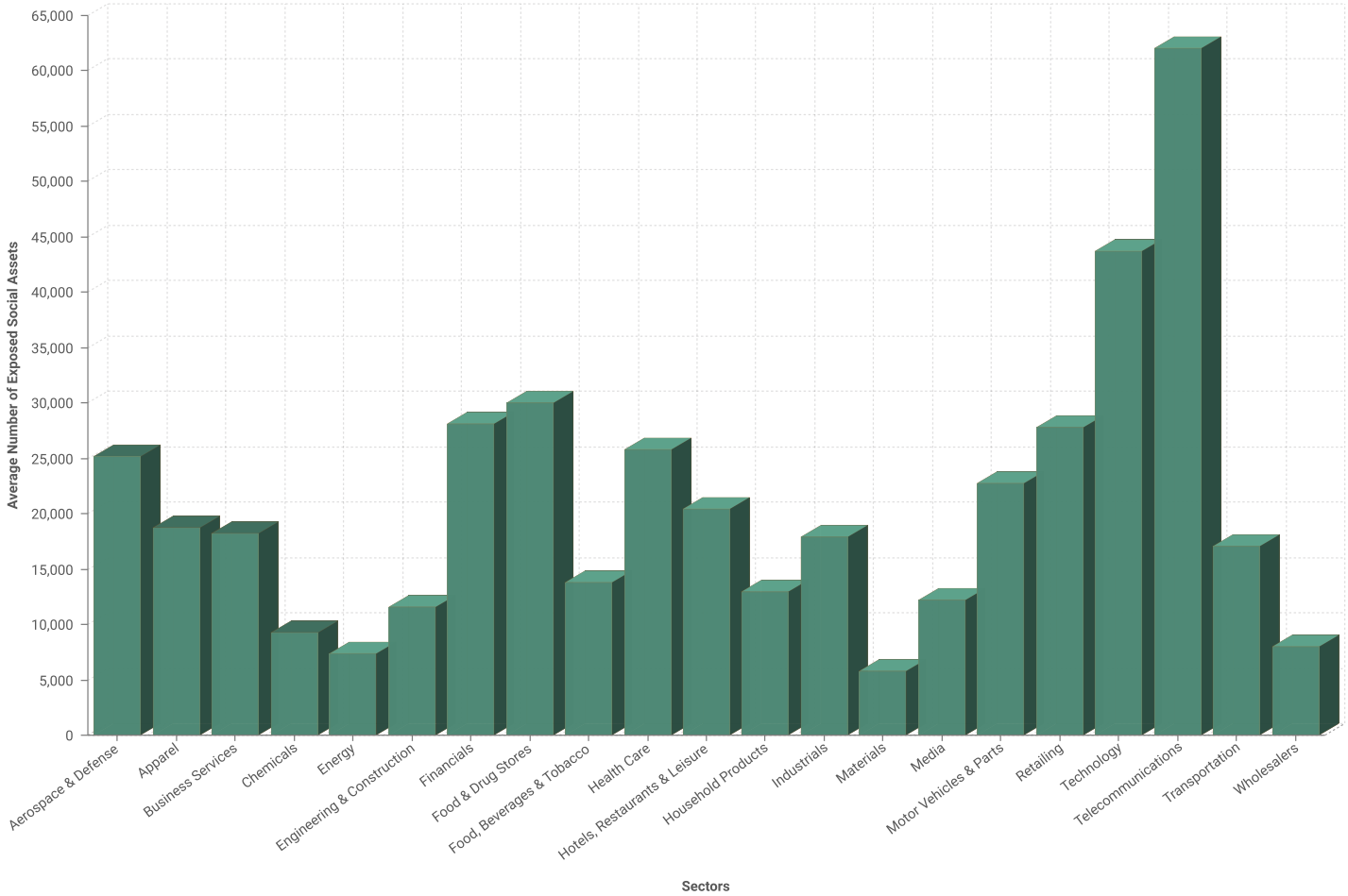
What It Is

Social assets include social media handles that may have been tied to the breached account.

How It Helps Criminals

Social assets can help criminals connect the dots between personal and corporate identities, which can be particularly useful in targeted attacks. An attacker may move laterally from one account to another, first compromising a social media account with limited protections in place and then using that access to compromise higher-value accounts or accounts belonging to the victim's trusted associates. Data shared on social media may also provide the attacker with insights that can aid in answering security questions or crafting believable spear phishing attacks.

Exposures by Sector: Average Number of Exposed Social Assets per Company



Asset Type: Account

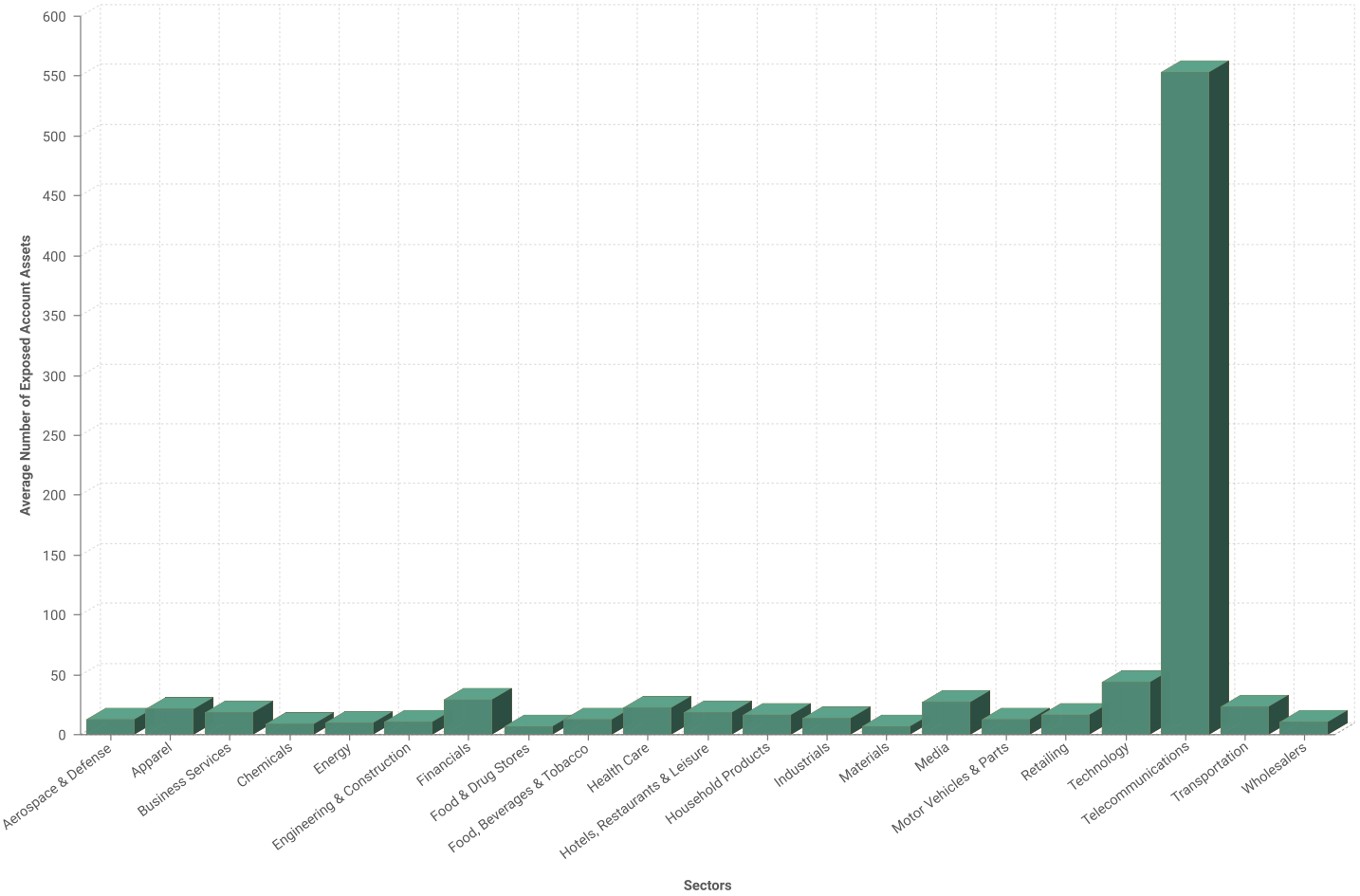
What It Is

Account assets are data related to the breached account itself—including secret answers to the security questions that many sites use as an extra layer of authentication. Account assets also encompass user activity records, such as the date an account was created and most recent login date.

How It Helps Criminals

Access to users' secret answers makes it easy for attackers to bypass authentication measures and take over accounts. In addition, criminals may use account activity records to engender trust and convince users to share additional information, such as their password. For example, an attacker might list recent actions a user has taken on specific dates and ask them to "verify" their validity by taking a risky action like clicking a phishing link.

Exposures by Sector: Average Number of Exposed Account Assets per Company



Fortune 1000 Breach Exposure by Sector

To provide additional insight into the breach exposure of the Fortune 1000, we have broken out our analysis by sector, using the sector classifications designated by *Fortune*.

23 COMPANIES FROM THE AEROSPACE INDUSTRY

1,226 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,802,275 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 78,360**

10,562,205 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 459,226

79% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

5,624,967 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 244,564

4,535,348 TOTAL OTHER ASSETS

Average Other Assets Per Company

Social	25,136
Phone	10,784
Geolocation	7,489
Financial	13
Other	153,766

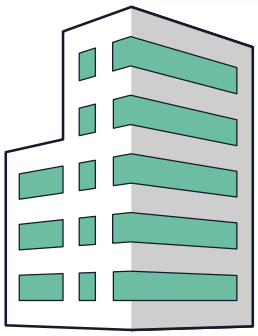
401,890 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

17,473 Average Number of Exposed Passwords per Company

1,651 Potentially Exposed C-Level Executives

44 Potentially Infected Employees



14 COMPANIES

FROM THE APPAREL INDUSTRY

878 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

678,647 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 48,475**

4,419,706 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 315,693

74% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

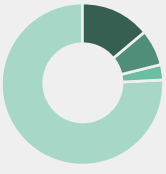
2,414,770 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 172,484

1,878,399 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	18,758
Phone	9,707
Geolocation	4,266
Financial	21
Other	101,420

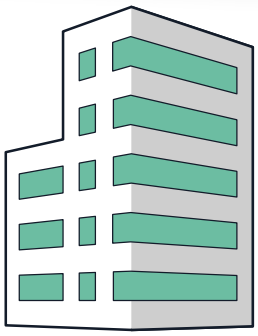
126,537 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

9,038 Average Number of Exposed Passwords per Company

1,555 Potentially Exposed C-Level Executives

33 Potentially Infected Employees



50 COMPANIES

SPANNING THESE INDUSTRY FIELDS

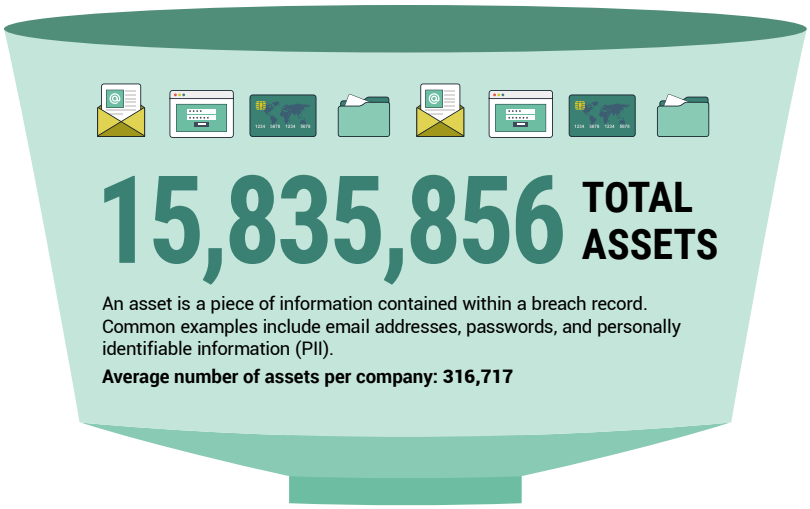
- Advertising, marketing
- Diversified Outsourcing Services
- Education
- Equipment Leasing
- Financial Data Services
- Miscellaneous
- Temporary Help
- Waste Management

1,441 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

2,444,662 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 48,893**



15,835,856 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 316,717

PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

8,693,196

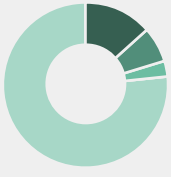
TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 173,864

6,716,168 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	18,203
Phone	9,224
Geolocation	4,201
Financial	18
Other	102,678

426,492 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

8,530 Average Number of Exposed Passwords per Company

6,823 Potentially Exposed C-Level Executives

123 Potentially Infected Employees

30 COMPANIES FROM THE CHEMICAL INDUSTRY

1,234 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

971,444 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 32,381**

5,718,227 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 190,608

77% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

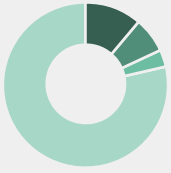
3,013,667 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 100,456

2,469,714 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	9,303
Phone	5,704
Geolocation	2,614
Financial	9
Other	64,694

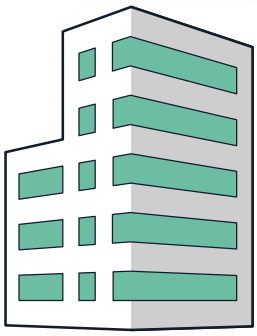
234,846 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

7,828 Average Number of Exposed Passwords per Company

1,457 Potentially Exposed C-Level Executives

17 Potentially Infected Employees



118 COMPANIES

SPANNING THESE INDUSTRY FIELDS

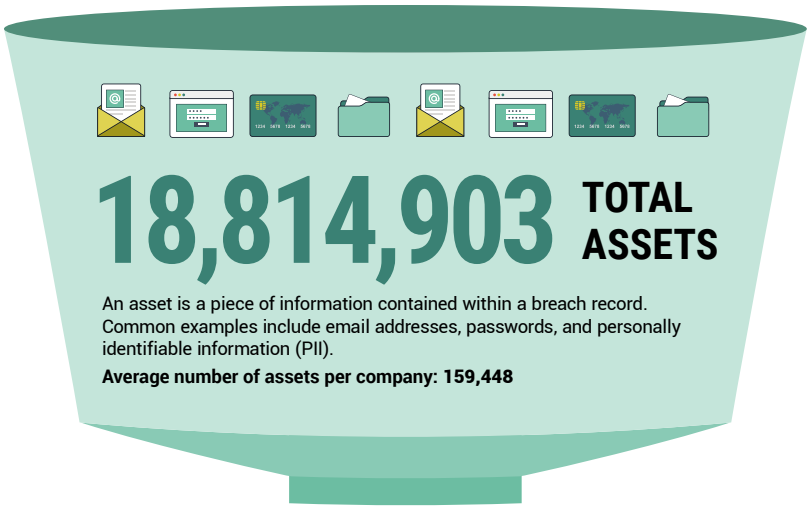
- Energy
- Mining, Crude-Oil Production
- Miscellaneous
- Oil and Gas Equipment, Services
- Petroleum Refining
- Pipelines
- Utilities: Gas and Electric

1,597 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

3,140,632 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 26,616**



18,814,903 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 159,448

PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

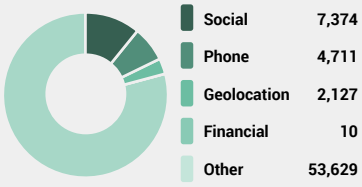
10,114,550 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 85,717

8,006,327 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	7,374
Phone	4,711
Geolocation	2,127
Financial	10
Other	53,629

694,026 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

5,882 Average Number of Exposed Passwords per Company

5,581 Potentially Exposed C-Level Executives

39 Potentially Infected Employees

31 COMPANIES

SPANNING THESE INDUSTRY FIELDS

Engineering • Construction • Homebuilding

1,088 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,029,116 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 33,197**

6,191,660 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 199,731

79% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

3,334,003 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 107,548

2,634,511 TOTAL OTHER ASSETS

Average Other Assets Per Company

Social	11,550
Phone	4,932
Geolocation	2,939
Financial	11
Other	65,552

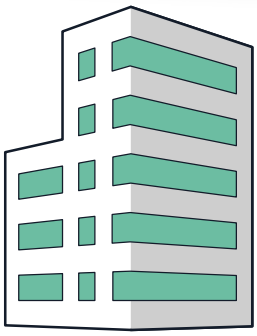
223,146 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

7,198 Average Number of Exposed Passwords per Company

3,125 Potentially Exposed C-Level Executives

32 Potentially Infected Employees



149
COMPANIES

SPANNING THESE INDUSTRY FIELDS

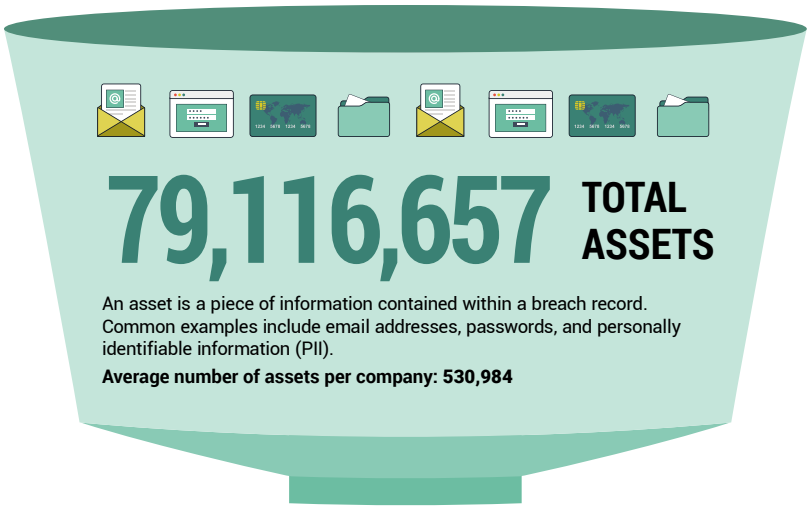
- Commercial Banks
- Diversified Financials
- Real Estate
- Securities
- Insurance: Life, Health (Mutual)
- Insurance: Life, Health (Stock)
- Insurance: Property and Casualty (Mutual)
- Insurance: Property and Casualty (Stock)

2,267 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

13,215,600 TOTAL BREACH RECORDS

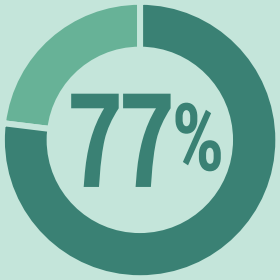
A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 88,695**



79,116,657 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 530,984



PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

42,626,828

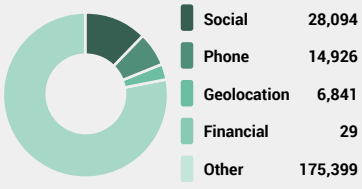
TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 286,086

33,568,223 TOTAL OTHER ASSETS

Average Other Assets Per Company



2,921,606 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

19,608 Average Number of Exposed Passwords per Company

36,414 Potentially Exposed C-Level Executives

146 Potentially Infected Employees

11 COMPANIES

SPANNING THESE INDUSTRY FIELDS

Grocery and Food Stores • Pharmacy and Drug Stores

508 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

904,742 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 82,249**

6,390,994 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 580,999

76% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

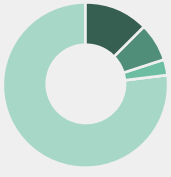
3,705,364 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 336,851

2,617,850 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	29,984
Phone	17,822
Geolocation	7,665
Financial	7
Other	182,509

67,780 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

6,162 Average Number of Exposed Passwords per Company

1,178 Potentially Exposed C-Level Executives

12 Potentially Infected Employees

36 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Beverage Products
- Food Production
- Food Consumer Products
- Tobacco Products

1,264 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,181,400 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 32,817**

7,855,489 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 218,208

74% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

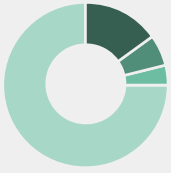
4,351,522 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 120,876

3,305,795 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	13,844
Phone	5,583
Geolocation	3,596
Financial	13
Other	68,792

198,172 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

5,505 Average Number of Exposed Passwords per Company

2,513 Potentially Exposed C-Level Executives

52 Potentially Infected Employees

72 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Insurance and Managed Care
- Medical Facilities
- Pharmacy and Other Services
- Medical Products and Equipment
- Pharmaceuticals
- Scientific, Photographic and Control Equipment
- Wholesalers

1,955 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

5,703,012 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 79,209**

35,645,538 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 495,077

80% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

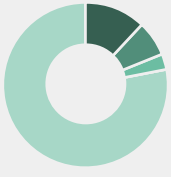
19,015,522 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 264,104

15,401,293 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	25,822
Phone	14,773
Geolocation	6,385
Financial	22
Other	166,905

1,228,723 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

17,066 Average Number of Exposed Passwords per Company

9,186 Potentially Exposed C-Level Executives

123 Potentially Infected Employees

27 COMPANIES

SPANNING THESE INDUSTRY FIELDS

Food Services • Hotels, Casinos & Resorts

1,092 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,723,981 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 63,851**

10,676,292 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 395,418

80% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

5,916,991 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 219,148

4,474,962 TOTAL OTHER ASSETS

Average Other Assets Per Company

Social	20,478
Phone	12,426
Geolocation	4,195
Financial	18
Other	128,622

284,339 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

10,531 Average Number of Exposed Passwords per Company

7,021 Potentially Exposed C-Level Executives

56 Potentially Infected Employees

27 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Home Equipment
- Furnishings
- Household and Personal Products
- Miscellaneous
- Toys
- Sporting Goods

1,422 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,174,019 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 43,482**

6,842,833 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 253,438

82% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

3,476,295 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 128,752

3,033,916 TOTAL OTHER ASSETS

Average Other Assets Per Company

Social	12,938
Phone	7,208
Geolocation	3,301
Financial	17
Other	88,904

332,622 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

12,319 Average Number of Exposed Passwords per Company

2,420 Potentially Exposed C-Level Executives

53 Potentially Infected Employees

49 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Construction and Farm Machinery
- Industrial Machinery
- Electronics, Electrical Equipment
- Miscellaneous

2,075 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

3,303,973 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 67,428**

17,639,665 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 359,993

77% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

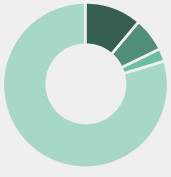
8,860,130 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 180,819

7,818,791 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	17,898
Phone	10,476
Geolocation	4,213
Financial	14
Other	126,966

960,744 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

19,607 Average Number of Exposed Passwords per Company

5,200 Potentially Exposed C-Level Executives

98 Potentially Infected Employees

47 COMPANIES

SPANNING THESE INDUSTRY FIELDS

- Building Materials, Glass
- Forest and Paper Products
- Metals
- Miscellaneous
- Packaging
- Containers

1,134 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

975,794 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 20,762**

6,171,322 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 131,305

77% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

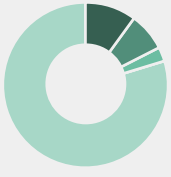
3,290,268 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 70,006

2,692,553 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	5,773
Phone	4,311
Geolocation	1,607
Financial	7
Other	45,590

188,501 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

4,011 Average Number of Exposed Passwords per Company

2,182 Potentially Exposed C-Level Executives

23 Potentially Infected Employees

26 COMPANIES

SPANNING THESE MEDIA FIELDS

Entertainment • Publishing • Printing

1,606 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

2,155,904 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 82,919**

8,995,511 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 345,981

85% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

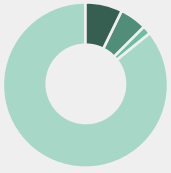
3,462,062 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 133,156

4,328,081 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	12,230
Phone	8,825
Geolocation	2,838
Financial	27
Other	142,544

1,205,368 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

46,360 Average Number of Exposed Passwords per Company

2,327 Potentially Exposed C-Level Executives

138 Potentially Infected Employees

23 COMPANIES

SPANNING THESE INDUSTRY FIELDS

Motor Vehicles & Parts Suppliers

1,557 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,334,710 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 58,031**

8,206,498 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 356,804

80% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

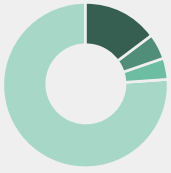
4,330,381 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 188,277

3,546,661 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	22,726
Phone	7,940
Geolocation	6,375
Financial	13
Other	117,148

329,456 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

14,324 Average Number of Exposed Passwords per Company

2,123 Potentially Exposed C-Level Executives

87 Potentially Infected Employees

73 COMPANIES

SPANNING THESE RETAIL FIELDS

- Automotive Retailing, Services
- General Merchandisers
- Internet Services and Retailing
- Specialty Retailers: Apparel
- Specialty Retailers: Other
- Wholesalers: Electronics and Office Equipment

1,415 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

4,899,443 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 67,116**

33,274,383 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 455,813

53% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

18,694,138 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 256,084

13,754,525 TOTAL OTHER ASSETS

Average Other Assets Per Company

Social	27,818
Phone	11,609
Geolocation	7,518
Financial	17
Other	141,455

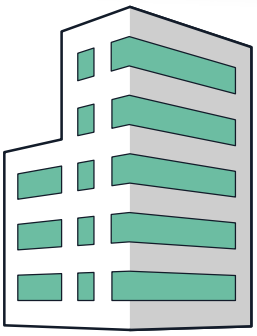
825,720 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

11,311 Average Number of Exposed Passwords per Company

10,877 Potentially Exposed C-Level Executives

196 Potentially Infected Employees



105
COMPANIES

SPANNING THESE TECH FIELDS

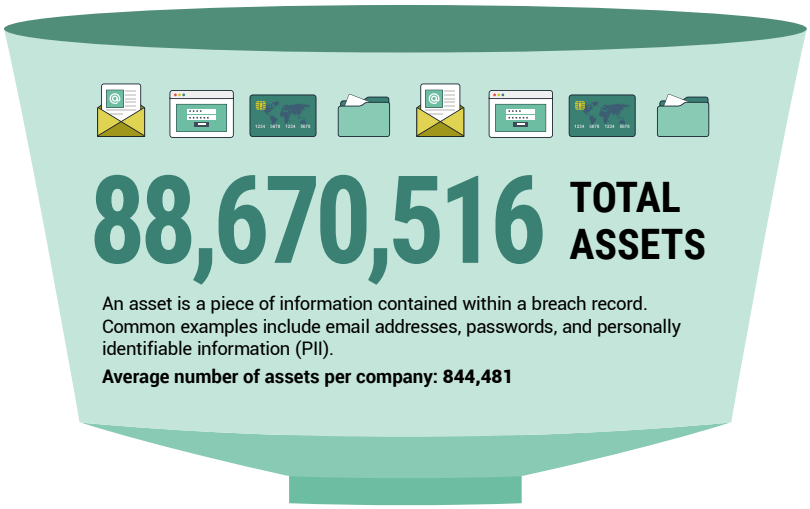
- Computer Software
- Computers, Office Equipment
- Information Technology Services
- Internet Services and Retailing
- Network and Other Communications Equipment
- Scientific, Photographic and Control Equipment
- Semiconductors and Other Electronic Components

3,701 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

17,633,056 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 167,934**



88,670,516 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 844,481

PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

40,603,797

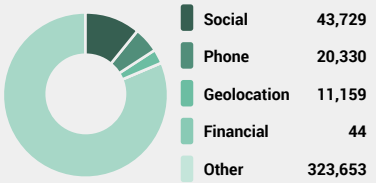
TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 386,703

41,886,029 TOTAL OTHER ASSETS

Average Other Assets Per Company



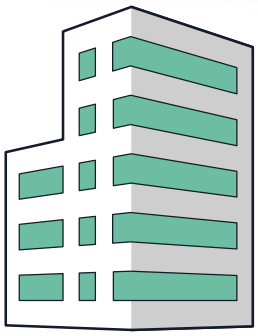
6,180,690 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

58,864 Average Number of Exposed Passwords per Company

15,468 Potentially Exposed C-Level Executives

1,022 Potentially Infected Employees



11 COMPANIES

FROM THE TELECOM INDUSTRY

2,318 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

8,654,158 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 786,742**

31,982,530 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 2,907,503

74% PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

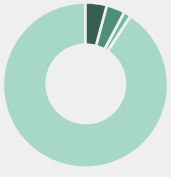
10,975,877 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 997,807

15,472,856 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	62,056
Phone	50,789
Geolocation	18,488
Financial	553
Other	1,274,736

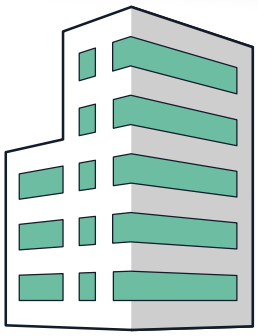
5,533,797 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

503,072 Average Number of Exposed Passwords per Company

2,346 Potentially Exposed C-Level Executives

357 Potentially Infected Employees



40
COMPANIES

SPANNING THESE TRANSPORT FIELDS

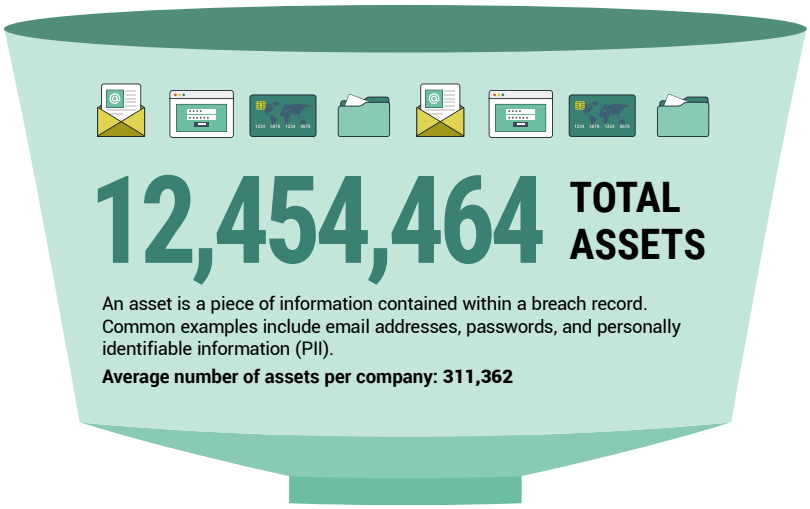
- Airlines
- Mail, Package, and Freight Delivery
- Railroads
- Shipping
- Transportation and Logistics
- Transportation Equipment
- Trucking, Truck Leasing

1,627 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

2,142,367 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 53,559**



12,454,464 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 311,362

PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

6,660,212

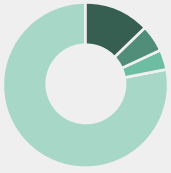
TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 166,505

5,285,432 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	17,027
Phone	7,145
Geolocation	5,154
Financial	23
Other	102,787

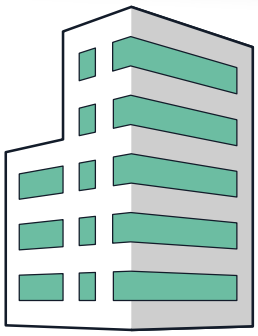
508,820 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

12,721 Average Number of Exposed Passwords per Company

4,609 Potentially Exposed C-Level Executives

76 Potentially Infected Employees



38 COMPANIES

SPANNING THESE WHOLESALE FIELDS

Wholesalers: Diversified

Wholesalers: Electronics and Office Equipment

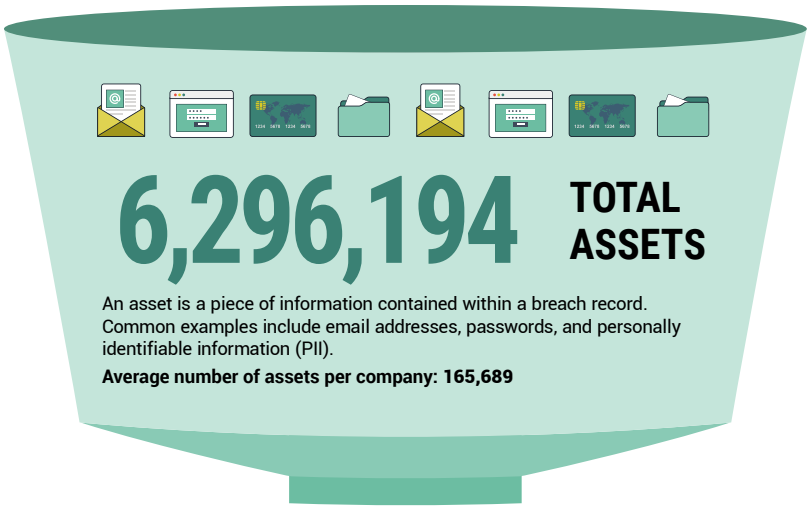
Wholesalers: Food and Grocery

1,063 TOTAL BREACH SOURCES

The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.

1,044,943 TOTAL BREACH RECORDS

A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 27,499**



6,296,194 TOTAL ASSETS

An asset is a piece of information contained within a breach record. Common examples include email addresses, passwords, and personally identifiable information (PII).

Average number of assets per company: 165,689

PASSWORD REUSE INDEX

A metric that measures how many of a company's employees have more than one credential exposure and have reused a password or a close variation across several sites.

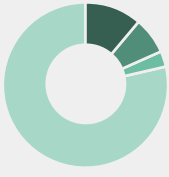
3,394,965 TOTAL PII ASSETS

Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 89,341

2,674,321 TOTAL OTHER ASSETS

Average Other Assets Per Company



Social	7,991
Phone	5,004
Geolocation	2,074
Financial	11
Other	55,297

226,908 TOTAL CORPORATE EXPOSED CREDENTIALS

Corporate credentials include pairings of corporate email addresses and plaintext (decrypted) passwords that are fully exploitable and ready for criminals to use.

5,971 Average Number of Exposed Passwords per Company

3,027 Potentially Exposed C-Level Executives

32 Potentially Infected Employees

Your Plan of Action

SpyCloud's analysis of Fortune 1000 companies' exposure as a result of third-party breaches has revealed more than 412 million breach assets in criminals' hands, 23.1 million of which are plaintext passwords tied to Fortune 1000 company employees. Combined with high rates of password reuse, these exposures represent significant account takeover risks for these organizations and the companies that do business with them.

Attackers actively test stolen credentials against different accounts to exploit bad password habits and gain access to corporate systems and data. Even worse, stolen PII and account data make it easy for criminals to craft highly targeted, creative attacks that cause great harm and are difficult to detect.

Enterprises must be able to trust the identities of the employees, consumers, and suppliers logging into their networks—and safeguard the corporate assets and IP behind those logins. The answer is to build early detection and remediation of exposed credentials into their cybersecurity strategy, and the best method, simply put, is to use SpyCloud.

Consumer ATO Prevention

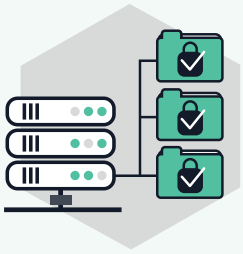
Protect your users from account takeover fraud and unauthorized purchases.

Learn More →

Employee ATO Prevention

Protect your organization from breaches and BEC due to password reuse.

Learn More →



Active Directory Guardian

Automatically detect and reset exposed Windows accounts.

Learn More →

Third Party Insight

Monitor third party exposures and share data to aid in remediation.

Learn More →

The SpyCloud Difference

Building a security program around technologies that proactively leverage data acquired through Human Intelligence (HUMINT) tradecraft very early in the breach timeline is a critical path to success. SpyCloud's solutions, backed by the world's largest repository of recovered stolen credentials and PII, enables enterprises to stay ahead of account takeover by detecting and automatically resetting compromised passwords early, before criminals have a chance to use them.

Our customers continue to tell us their ability to prevent account takeover hinges both on access to relevant data (including the most plaintext passwords in the industry) and in being able to make that data operationally actionable through automation.

Visit spycloud.com to see your domain's real-time breach exposure details, powered by SpyCloud data, and learn more about our account takeover prevention solutions.