



SpyCloud

2021 Report:
**Breach Exposure of the
Fortune 1000**

SpyCloud

2021 Report: Breach Exposure of the Fortune 1000

[Overview](#)

[Key Findings](#)

[At a Glance: Breach Exposure of the Fortune 1000](#)

[Corporate Credential Exposure of the Fortune 1000](#)

[Exposed Corporate Credentials by Sector](#)

[Password Reuse: Worst Offenders by Sector](#)

[Favorite Passwords of Fortune 1000 Employees](#)

[Credentials Collected by Malware](#)

[Other Breach Exposures by Asset Type](#)

[Breach Exposure by Sector](#)

[Aerospace & Defense](#)

[Apparel](#)

[Business Services](#)

[Chemicals](#)

[Energy](#)

[Engineering & Construction](#)

[Financials](#)

[Food & Drug Stores](#)

[Food, Beverages & Tobacco](#)

[Health Care](#)

[Hotels, Restaurants & Leisure](#)

[Household Products](#)

[Industrials](#)

[Materials](#)

[Media](#)

[Motor Vehicles & Parts](#)

[Retailing](#)

[Technology](#)

[Telecommunications](#)

[Transportation](#)

[Wholesalers](#)

Overview

Given the explosion of digital services in recent years and the global shift to remote work in 2020, most people are juggling more online logins than ever. It's no wonder that users commonly fall back on weak and reused passwords that are easy to remember—and just as easy for criminals to exploit.

For enterprises, bad password hygiene puts sensitive corporate assets within easy reach of malicious actors. Even at America's largest companies, a data breach that reveals an employee's reused password or personal information can help a criminal sidestep sophisticated security measures and gain privileged access to corporate resources. Each new breach provides bad actors with more stolen data to exploit.

For the second year in a row, SpyCloud has analyzed our entire database to demonstrate the scope of breach exposure affecting large enterprises, specifically looking at the breach exposure of the Fortune 1000. With well over 100 billion breach assets collected to date, SpyCloud maintains the industry's largest repository of recovered stolen credentials and PII, collected as quickly as possible after a breach using human intelligence. SpyCloud researchers closely monitor the criminal underground for stolen data that has fallen into criminals' hands, helping enterprise customers protect vulnerable users and stay a step ahead of bad actors.

To perform our analysis, 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, such as example@employer.com, we were able to tie the resulting breach record to their employer.

This analysis excludes breach data tied to corporate employees' personal aliases, which can also be tied to corporate identities and used for illicit gain. It will include 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.

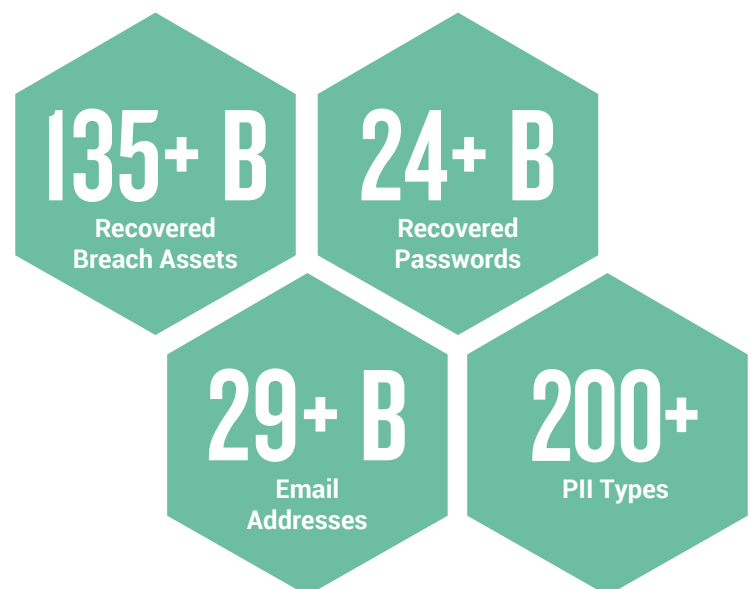
This year, we found over 543 million breach assets within our dataset tied directly to Fortune 1000 employee emails, a 29% increase from last year's report. To demonstrate the threat that this data poses to enterprise security, this analysis addresses the data both by asset type and by sector, as defined by Fortune.

About SpyCloud Data

Truly Actionable Breach Data to Prevent Account Takeover

SpyCloud uses Human Intelligence (HUMINT) to quickly recover breach data, often within days of the breach occurring. Our unique data cleansing and password cracking process reveals compromised credentials faster and with greater match rates. Access to this massive breach database enables enterprises to quickly identify and take action on exposed accounts, preventing those exposures from progressing to account takeovers. SpyCloud safeguards more than 2 billion employee and consumer accounts from account takeover and follow-on attacks like credit card fraud, phishing, and ransomware.

[Learn more at spycloud.com.](https://www.spycloud.com)



Key Findings

1. The volume of breach data tied to Fortune 1000 employees is staggering.

Overall, we found over 543 million breach assets tied to Fortune 1000 employees, a 29% increase from last year. Across all industries, nearly 26 million plaintext passwords belonging to Fortune 1000 employees are available to cybercriminals, which means an average of 25,927 exposed passwords per company (a 12% increase from last year).



2. Even among Fortune 1000 employees, password reuse across multiple accounts remains rampant.

For obvious reasons, we can't test exposed passwords to find out which ones have been reused at work. However, across all employees with more than one password exposed, we saw a 76.7% rate of password reuse. If employees reuse passwords this frequently outside of work, it's likely that many have recycled their corporate logins as well.

3. Telecommunications and Technology companies have the most exposed corporate credentials and potentially infected employees.

In total, the Technology sector has the most exposed credentials (6.7 million) and by far the largest number of potentially infected employees (13,897). Telecommunications comes next by total count (6 million and 2,328 respectively). Averaged out per company, however, the Telecommunications sector fares the worst in both categories, with an average of 552,601 exposed credentials and 212 potentially infected employees per company, compared to 61,747 and 127 respectively per Technology company.








4. In the context of 2020 supply chain breaches, bad passwords in Aerospace & Defense raised our eyebrows.

While company names are popular password choices across all sectors, it's unnerving to see the names of major defense contractors pop up as popular employee passwords—particularly when you consider that these breaches come from third-party sites. Six of the top 10 most popular passwords of the Aerospace & Defense sector include company names.

5. Credentials for 133,927 Fortune 1000 C-level executives are available to criminals—and 29% are from the Financials sector.

The Financial Sector alone has over 39,328 exposed C-level executives. On average, however, the Hotels, Restaurants & Leisure sector has the most exposed executives per company: 320 per company, versus 243 per company in the Financials sector.

At a Glance: Breach Exposure of the Fortune 1000

18,280	TOTAL BREACH SOURCES Total number of breaches in the SpyCloud dataset that include records tied to Fortune 1000 corporate email addresses.	
107,552,781	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.	
543,802,413	TOTAL BREACH ASSETS A breach asset is a piece of information contained within a breach record. Ex: a password, an address, a phone number.	
25,927,476	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.	
133,927	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 .	
76.7%	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.	
28,201	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 nearly 26 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	22	542,431	24,656
Apparel	16	143,339	8,959
Business Services	52	454,699	8,744
Chemicals	27	313,289	11,603
Energy	109	803,702	7,373
Engineering & Construction	30	245,286	8,176
Financials	162	3,383,948	20,889
Food & Drug Stores	10	50,052	5,005
Food, Beverage & Tobacco	37	259,588	7,016
Health Care	71	1,461,070	20,578
Hotels, Restaurants & Leisure	27	340,500	12,611
Household Products	26	342,699	13,181
Industrials	50	1,151,118	23,022
Materials	46	233,691	5,080
Media	25	1,311,295	52,452
Motor Vehicles & Parts	22	370,262	16,830
Retailing	75	898,662	11,982
Technology	109	6,730,415	61,747
Telecommunications	11	6,078,607	552,601
Transportation	38	562,201	14,795
Wholesalers	35	250,622	7,161
Total	1000	25,927,476	25,927

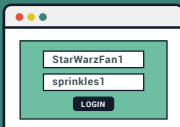
Password Reuse: Worst Offenders by Sector

Password reuse is rampant. An analysis of the SpyCloud database found a 60% password reuse rate among email addresses in our database exposed in more than one breach in 2020. That rate is even worse for employees of the Fortune 1000; though you can imagine the stakes (and security measures) are especially high, we found an average password reuse rate of 76.7%.

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 aaron431 [company name]lo
parker 456a33 research 12345 [redacted]off
[company name] password1 abc123 pass1
[company name] 123456789 12345678 1234
sunshine 111111 welcome [redacted]cd
[redacted]dork [redacted]cc [redacted]ce
[redacted]cb qwerty passport 10pace old123ma
[company name]5 unknown michael summer
1234567 welcome1 [company name] Password
baseball maggie Password1 bailey princess
[company name]1 student charlie passw0rd
jordan harley madison [company name] buster
monkey shadow michael1 hannah hunter
football newmember 19weed taylor matthew
jennifer Welcome1 24crow andrew 59mile
soccer tigger 59trick 1qaz2wsx michelle
letmein 123456a jessica zaq12wsx mustang
joshua jackson jesus1 jordan23 66bob ginger
ashley nicole pepper 123123 justin morgan
123abc vacation mickey nicholas 13pass13
    
```

In the SpyCloud database, we found:

Rank	Sector	Password Reuse Index
1	Media	85%
2	Household Products	82%
3	Hotels, Restaurants & Leisure	80%
4	Healthcare	79%
5	Motor Vehicles & Parts	79%
6	Aerospace & Defense	78%
7	Business Services	78%
8	Engineering & Construction	78%
9	Transportation	78%
10	Chemicals	77%
11	Financials	77%
12	Industrials	77%
13	Energy	76%
14	Materials	76%
15	Technology	76%
16	Telecommunications	76%
17	Food, Beverage & Tobacco	75%
18	Apparel	74%
19	Food & Drug Stores	73%
20	Wholesalers	73%
21	Retailing	65%

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 'PasswOrd!' 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 75,287 TIMES

THE PASSWORD

password

APPEARED 61,762 TIMES

THE PASSWORD

aaron431

APPEARED 36,775 TIMES

Credentials Collected by Malware

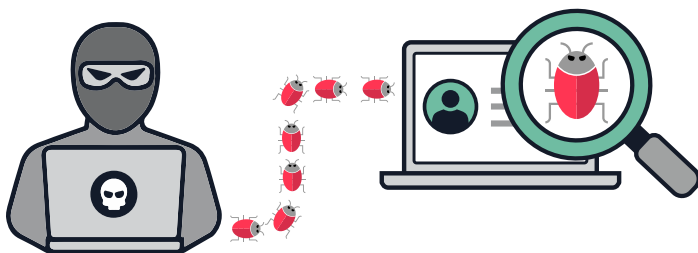
The Danger of Infected Employees

Not all of the exposed data in this report comes from data breaches. SpyCloud also recovers some information collected by botnets. Malware with keylogging components, or “stealers,” can siphon information such as browser history, autocomplete data, cookies, screenshots, system information, crypto wallets, and login credentials from an unsuspecting user’s infected system.

Like breach data, information stolen by botnets is collected by cybercriminals, shared in small circles, and sometimes posted on hacking web forums. When SpyCloud is able to recover some of these bot logs, we parse out the infected victim’s username, URL, and password in order to help consumers and organizations protect themselves. For this report, we searched these records for Fortune 1000 corporate email addresses to identify employees who may be using infected personal or corporate systems.

In total, SpyCloud has identified 28,201 potentially-infected Fortune 1000 employees, an average of 28 infected employees per company.

The breadth of data captured by these infections can have disastrous consequences for enterprises, whether the affected device is personal or corporate. Malware with keylogging components can record the employee’s every move, capturing browser history, files, system information, and login data for corporate and third-party resources. Bad actors can use this information to bypass multi-factor authentication, log into corporate networks, steal sensitive data, authorize fraudulent transactions, and more. Even without exact corporate logins, criminals can easily blackmail, extort, trick, or impersonate the victim to extend their access to corporate resources.



In the SpyCloud database, we found:

Fortune 1000 Sector	Potentially Infected Employees
Aerospace & Defense	173
Apparel	268
Business Services	891
Chemicals	223
Energy	543
Engineering & Construction	332
Financials	1,646
Food & Drug Stores	98
Food, Beverage & Tobacco	445
Health Care	1,120
Hotels, Restaurants & Leisure	450
Household Products	319
Industrials	1,018
Materials	202
Media	1,046
Motor Vehicles & Parts	632
Retailing	1,652
Technology	13,897
Telecommunications	2,328
Transportation	683
Wholesalers	235
Total	28,201

What About Infected Consumers?

In addition to infected employees, we also identified over 11 million potentially-infected consumers of Fortune 1000 services. These are users of Fortune 1000 consumer-facing sites where botnet logs show that they were infected while entering their username and password on the login page (e.g. jim@hotmail.com was infected while logging into signin.fortune1000company.com).

Because of the scope of this report, the true number of infected consumers for these sectors is likely higher; for example, we excluded many consumer-only domains from this analysis. We've also nixed credentials with usernames instead of email addresses because it's unclear whether they are employee or consumer records. However, each one of these infected consumers is at extremely high risk of account takeover, identity theft, and online fraud, which can result in substantial losses and brand damage for affected enterprises.

Here are just a few ways cybercriminals exploit consumers' stolen information:

- ❗ **Transfer funds from crypto wallets, investment portfolios, payment applications, and other accounts**
- ❗ **Place fraudulent orders using credit card information or gift cards stored within accounts**
- ❗ **Siphon loyalty points associated with accounts**
- ❗ **Commit warranty fraud using stored device information**
- ❗ **Change shipping addresses to facilitate package theft and drop-shipping**
- ❗ **Stalk or blackmail victims using browser history and other stolen data**
- ❗ **Sell login details and browser fingerprints to other criminals**

In the SpyCloud database, we found:

Fortune 1000 Sector	Potentially Infected Consumers
Aerospace & Defense	357
Apparel	30,432
Business Services	834,021
Chemicals	1,504
Energy	10,806
Engineering & Construction	2,527
Financials	27,464
Food & Drug Stores	24,798
Food, Beverage & Tobacco	9,508
Health Care	16,173
Hotels, Restaurants & Leisure	39,888
Household Products	11,276
Industrials	5,612
Materials	291
Media	1,081,080
Motor Vehicles & Parts	5,771
Retailing	1,058,973
Technology	7,812,321
Telecommunications	59,669
Transportation	25,132
Wholesalers	2,023
Total	11,059,626

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 entry point 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.

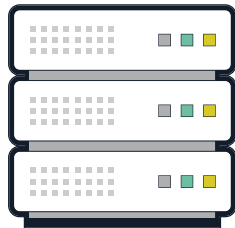
Criminals may engage in [highly-targeted, manual attacks](#) against victims with privileged access to corporate resources, such as C-suite leaders, senior executives, system administrators, and

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.

In total, SpyCloud has collected 543,802,413 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.

BREACH SOURCES



BREACH RECORDS

ASSETS



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

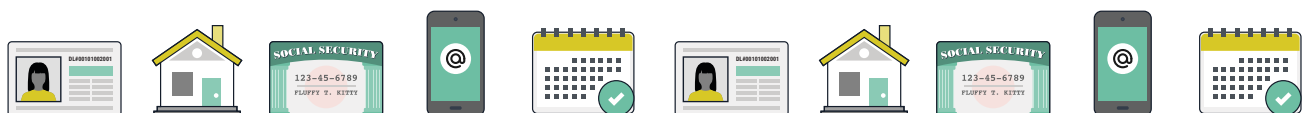
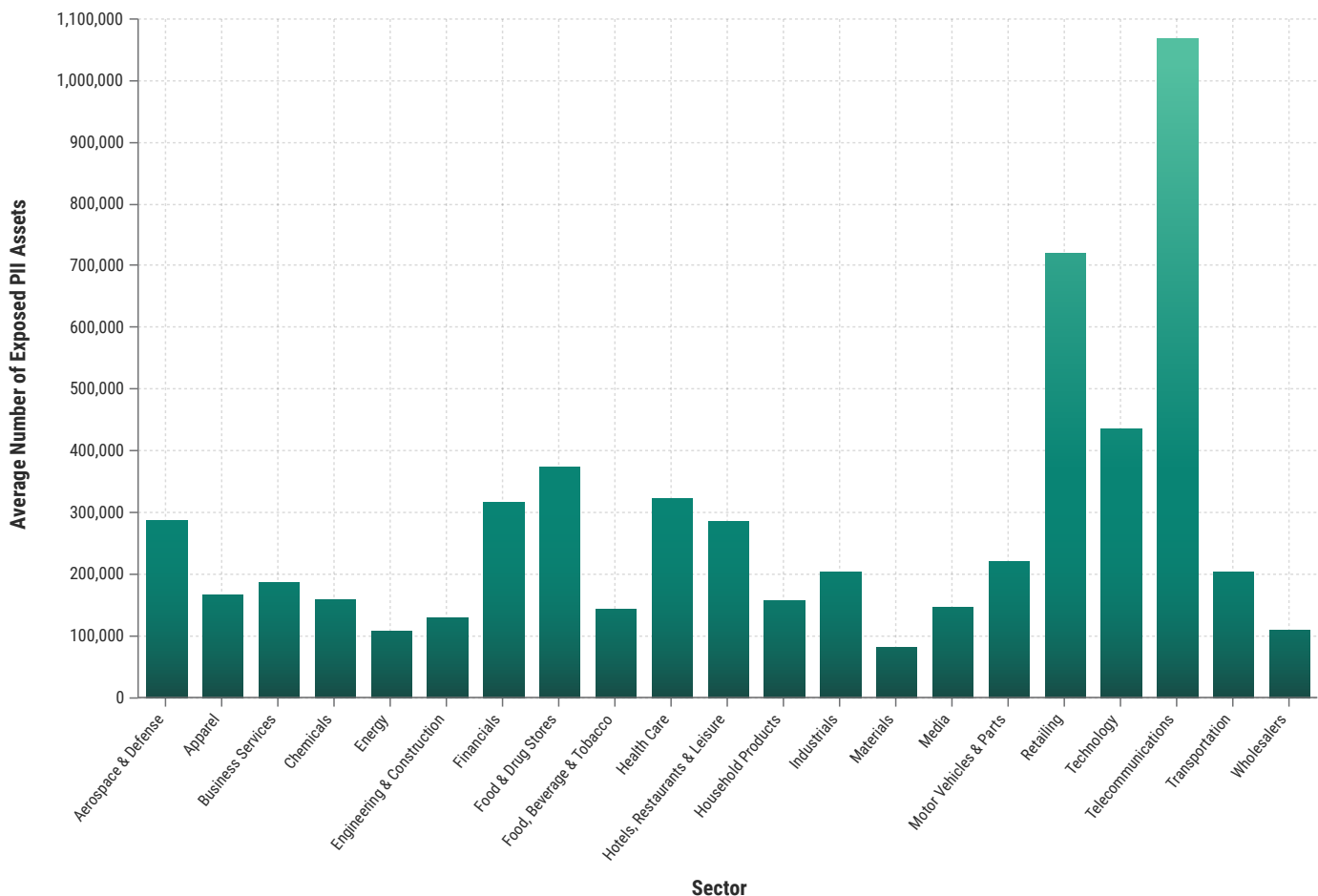
Personally identifiable information (PII) is data that could be used to identify an individual person. For the purposes of this report, SpyCloud has excluded some forms of PII that have been broken out into separate categories below, such as phone and financial assets. However, this category includes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

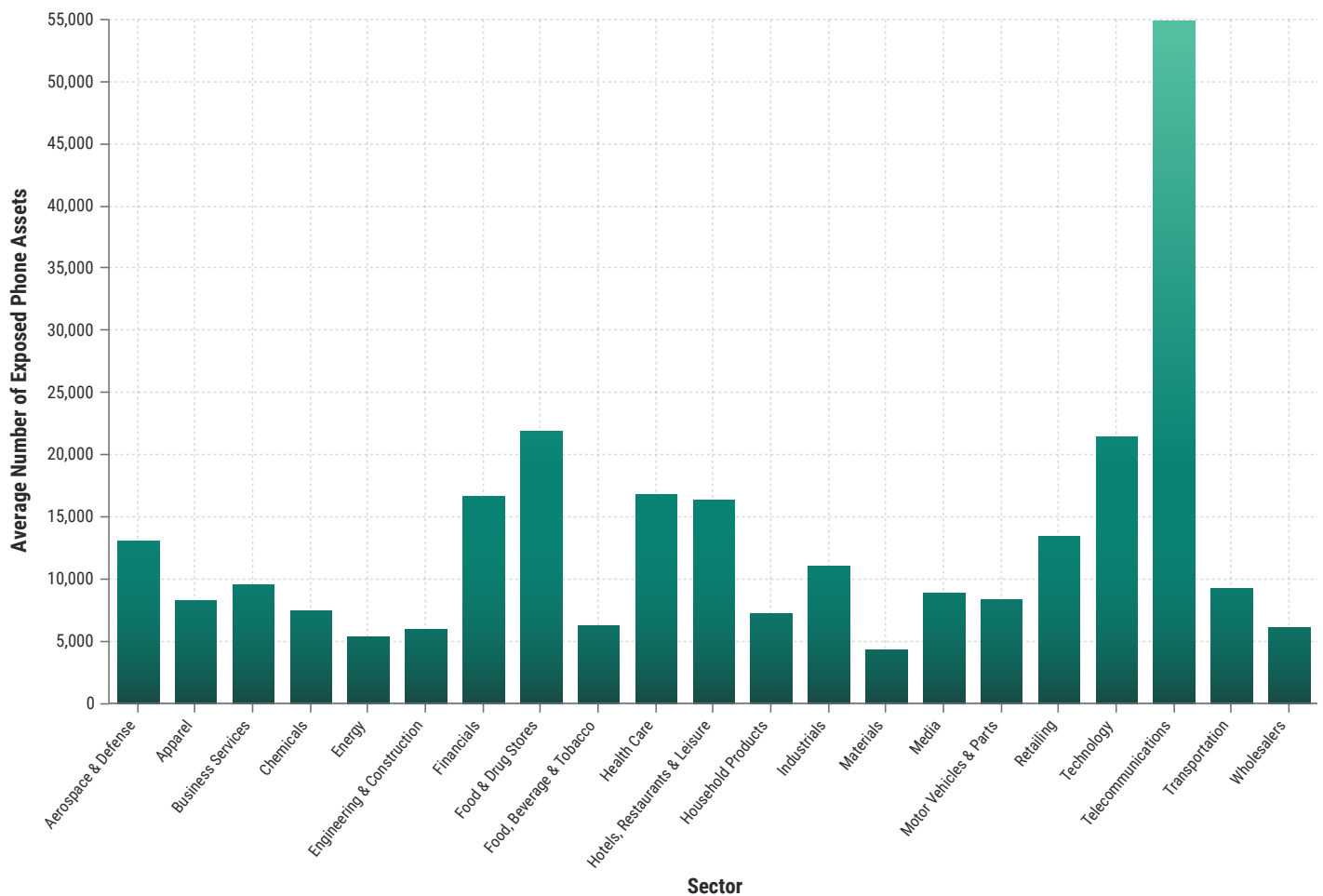
Phone assets are stolen phone numbers.

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.

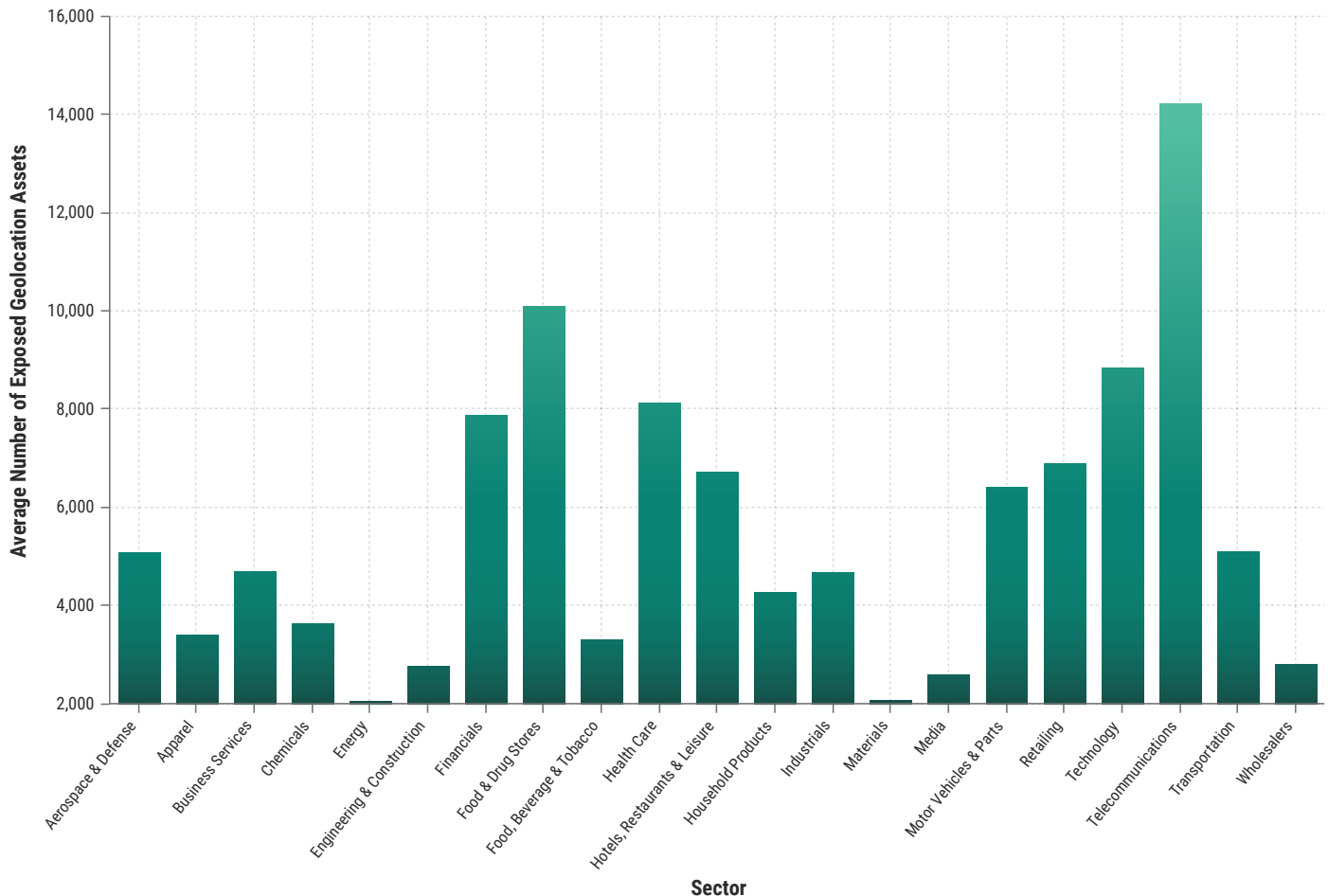
How It Helps Criminals

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.

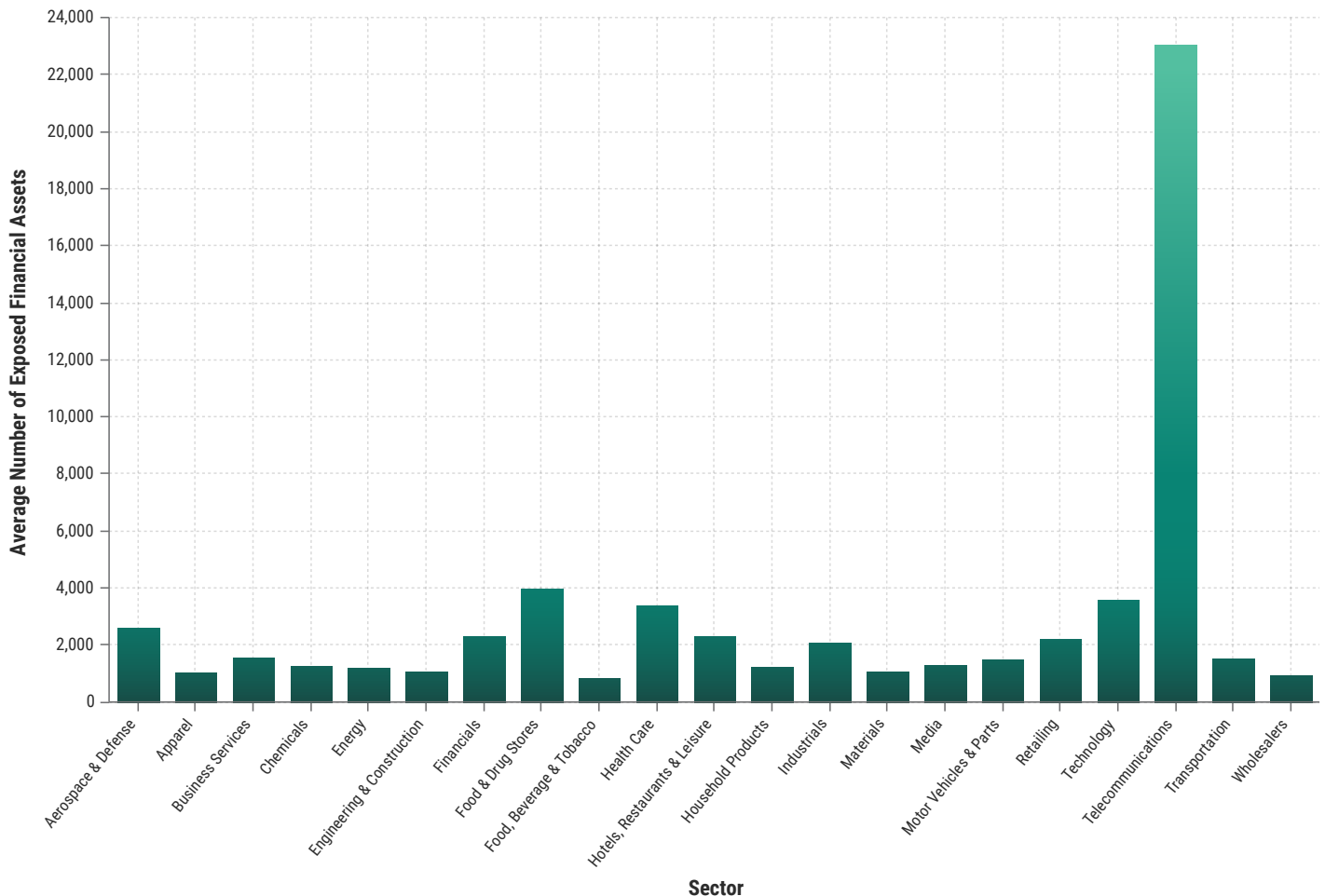


How It Helps Criminals

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

- ✓ Make fraudulent purchases
- ✓ Drain funds from accounts
- ✓ Resell card numbers to other criminals
- ✓ Collect victims' tax refunds

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



Asset Type: Social

What It Is

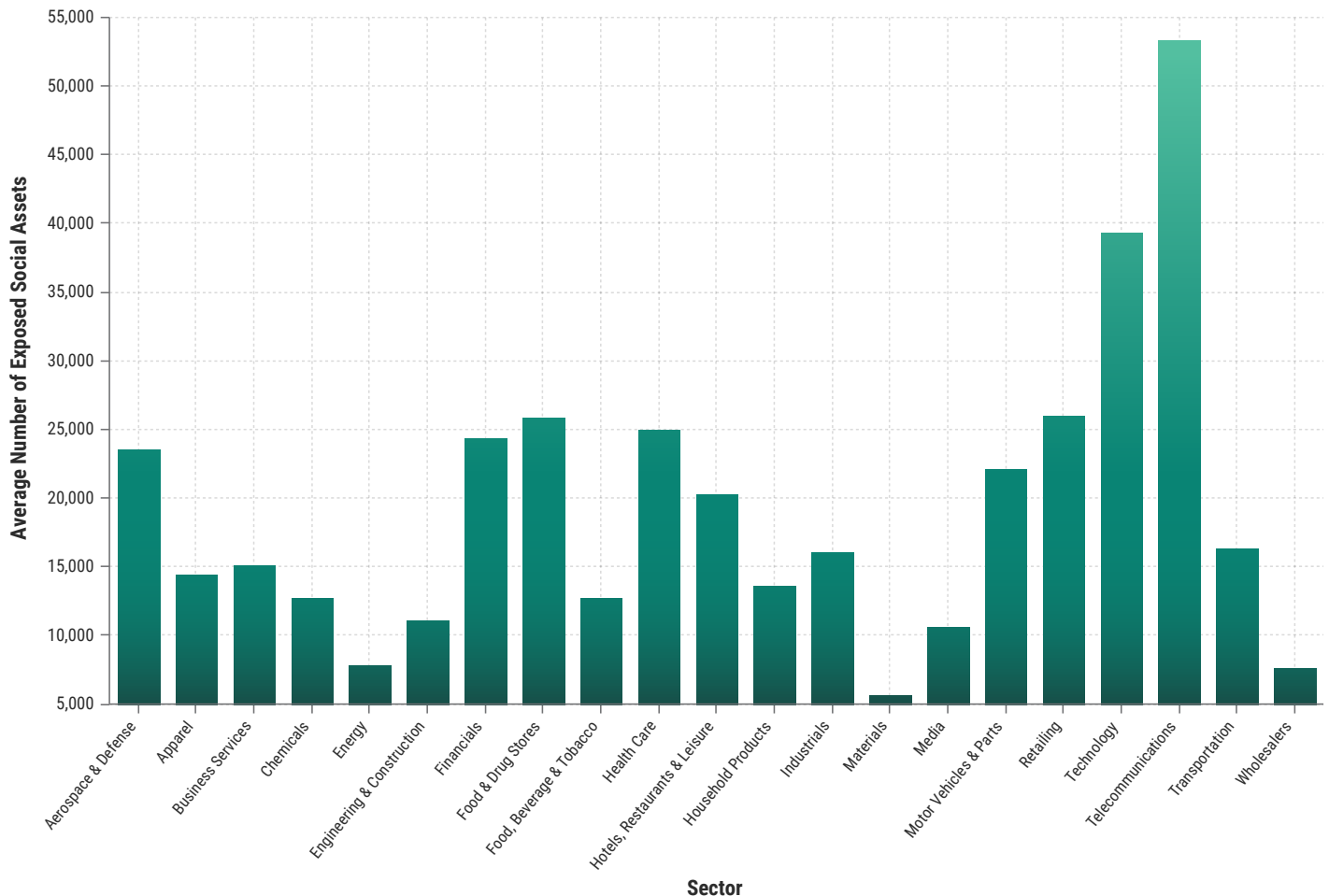
Social assets include social media handles that may have been tied to the breached account.



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



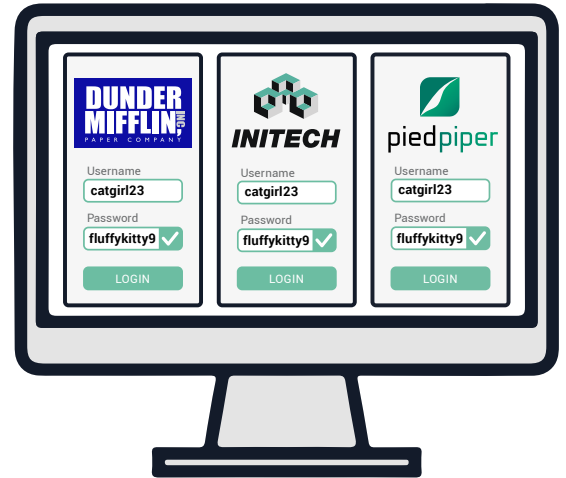
Asset Type: Account

What It Is

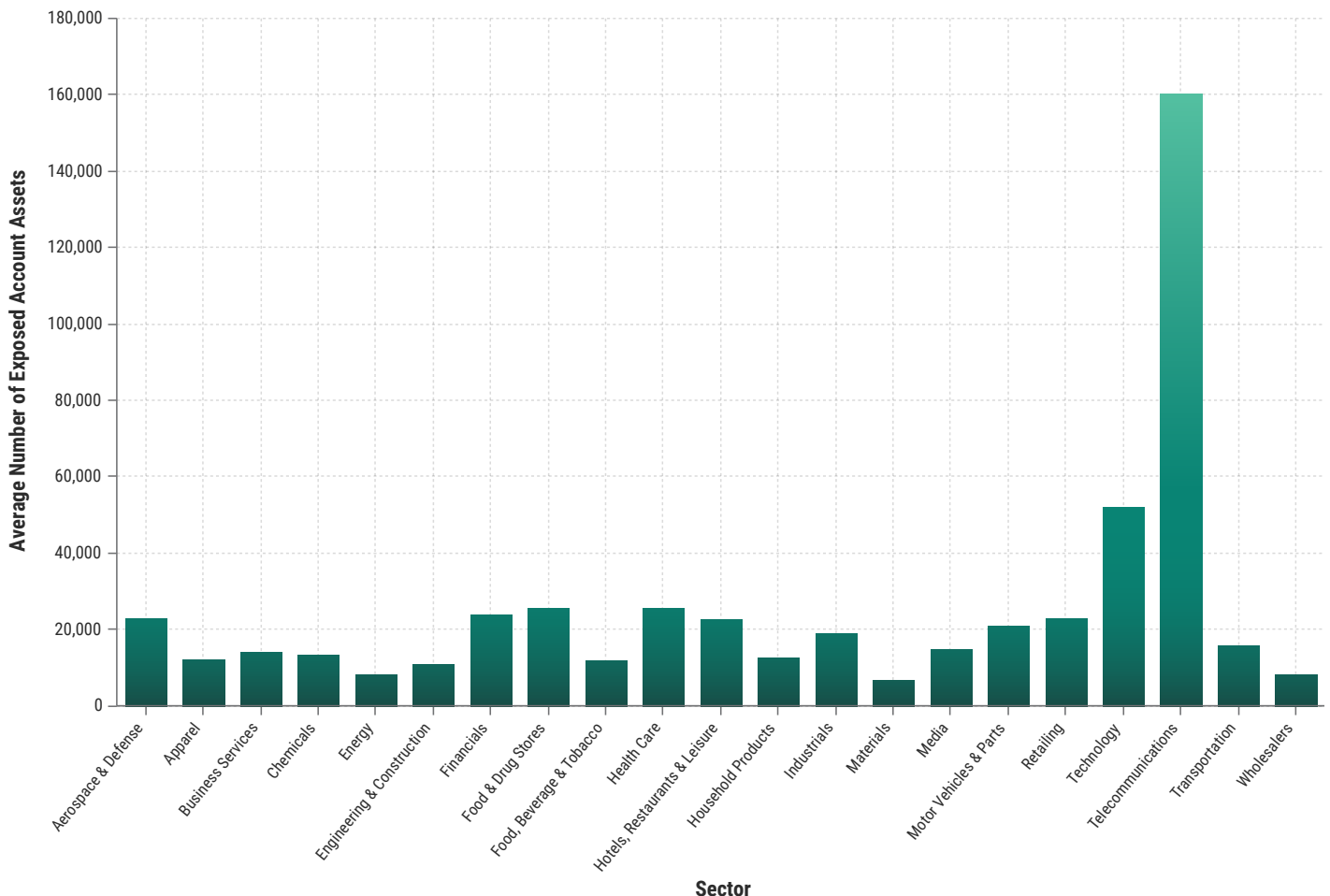
Account assets are data related to the breached account itself—including secret answers to the security questions that many sites use as an extra layer of authentication. Account assets also encompass user activity records, such as the date an account was created and most recent login date.

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*.

[Aerospace & Defense](#)

[Household Products](#)

[Apparel](#)

[Industrials](#)

[Business Services](#)

[Materials](#)

[Chemicals](#)

[Media](#)

[Energy](#)

[Motor Vehicles & Parts](#)

[Engineering & Construction](#)

[Retailing](#)

[Financials](#)

[Technology](#)

[Food & Drug Stores](#)

[Telecommunications](#)

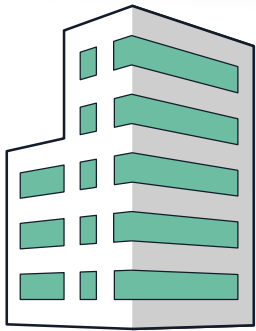
[Food, Beverages & Tobacco](#)

[Transportation](#)

[Health Care](#)

[Wholesalers](#)

[Hotels, Restaurants & Leisure](#)



22
COMPANIES

FROM THE AEROSPACE INDUSTRY



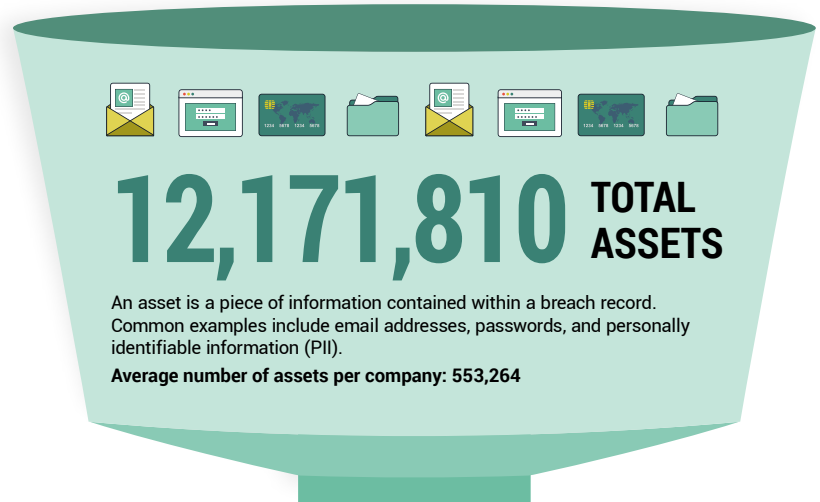
3,364 **TOTAL BREACH SOURCES**

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



2,445,973 **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: 111,181**



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.



6,326,968

TOTAL PII ASSETS

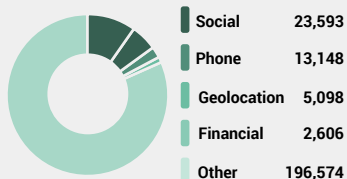
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 287,589



5,302,411 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



542,431

TOTAL CORPORATE EXPOSED CREDENTIALS

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

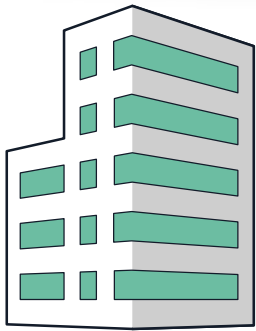


24,656 **Average Number of Exposed Passwords per Company**

1,595 **Potentially Exposed C-Level Executives**



173 **Potentially Infected Employees**



16
COMPANIES

FROM THE APPAREL INDUSTRY



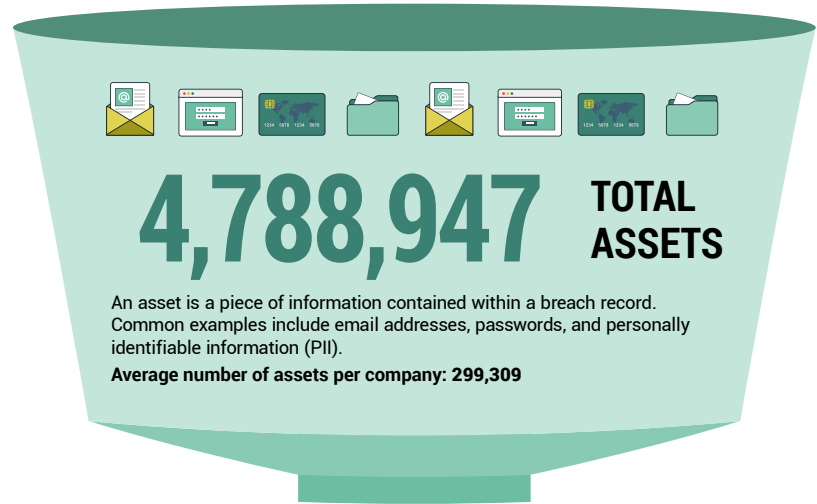
2,412 TOTAL BREACH SOURCES

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



839,022 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: 52,439**



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.



2,676,775

TOTAL PII ASSETS

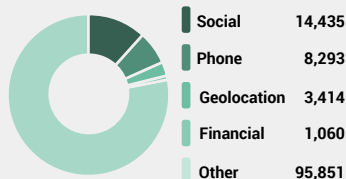
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 167,298



1,968,833 TOTAL OTHER ASSETS

Average Other Assets Per Company



143,339

TOTAL CORPORATE EXPOSED CREDENTIALS

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

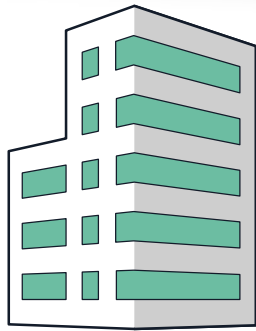


8,959 Average Number of Exposed Passwords per Company

1,600 Potentially Exposed C-Level Executives



268 Potentially Infected Employees



52
COMPANIES

SPANNING THESE INDUSTRY FIELDS

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



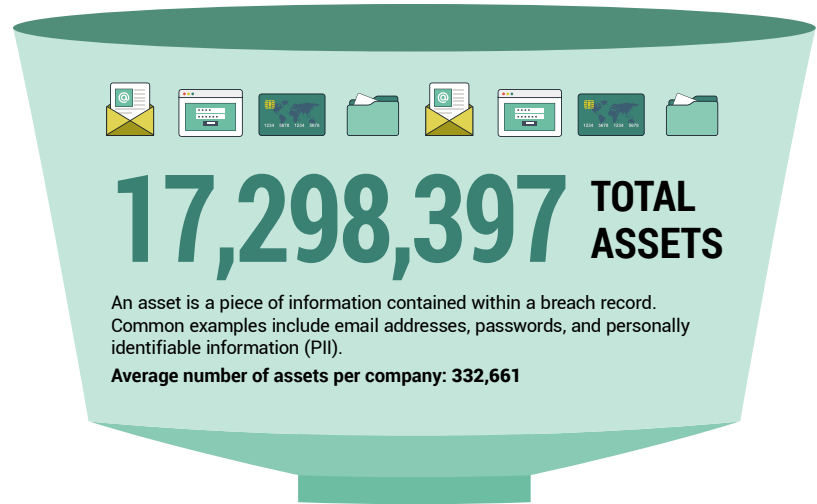
4,335 **TOTAL BREACH SOURCES**

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



3,010,428 **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: 57,893**



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.



9,742,678

TOTAL PII ASSETS

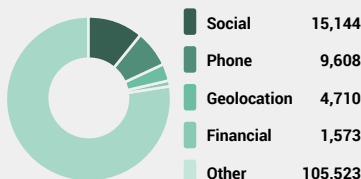
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 187,359



7,101,020 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



454,699

TOTAL CORPORATE EXPOSED CREDENTIALS

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

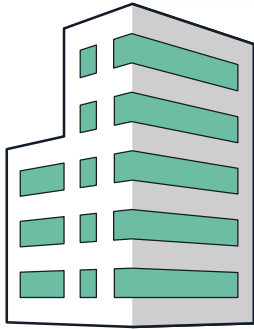


8,744 **Average Number of Exposed Passwords per Company**

6,156 **Potentially Exposed C-Level Executives**



891 **Potentially Infected Employees**



27
COMPANIES

FROM THE CHEMICAL INDUSTRY



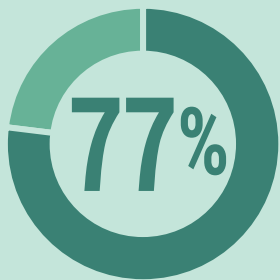
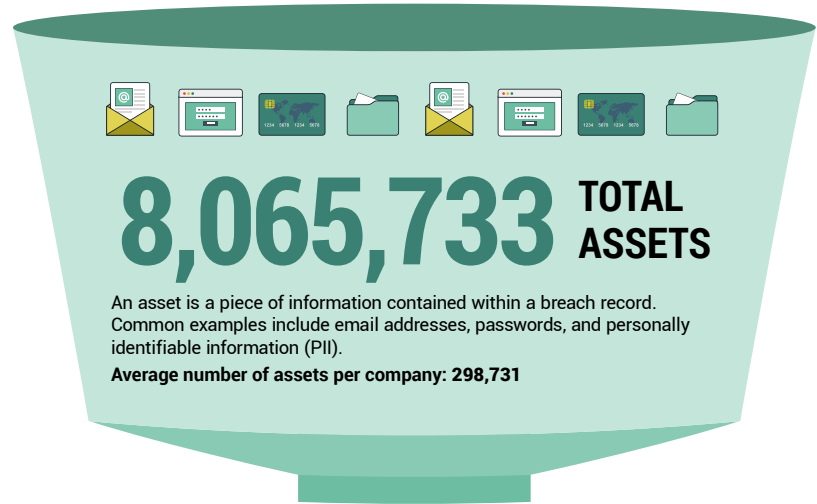
4,157 **TOTAL BREACH SOURCES**

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



1,557,285 **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: 57,677**



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.



4,329,283

TOTAL PII ASSETS

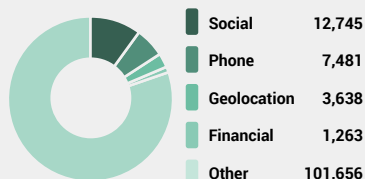
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 160,344



3,423,161 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



313,289

TOTAL CORPORATE EXPOSED CREDENTIALS

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

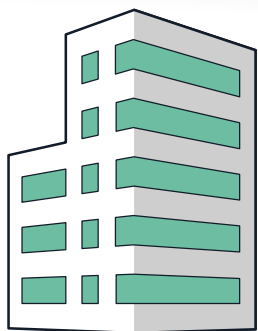


11,603 **Average Number of Exposed Passwords per Company**

1,707 **Potentially Exposed C-Level Executives**



223 **Potentially Infected Employees**



109
COMPANIES

SPANNING THESE INDUSTRY FIELDS

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



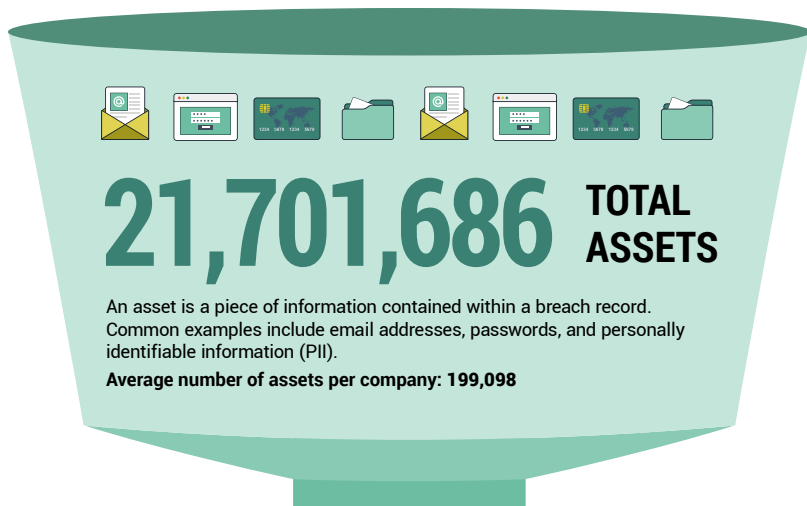
5,001 **TOTAL BREACH SOURCES**

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



4,132,691 **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: 37,915**



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.



11,768,661

TOTAL PII ASSETS

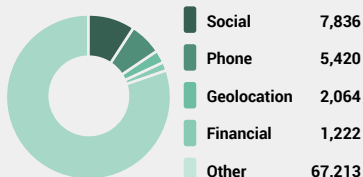
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 107,969



9,129,323 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



803,702

TOTAL CORPORATE EXPOSED CREDENTIALS

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

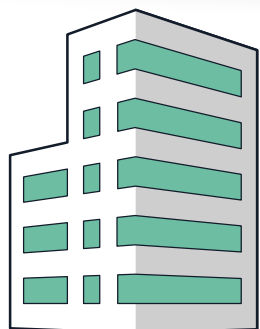


7,373 **Average Number of Exposed Passwords per Company**

5,697 **Potentially Exposed C-Level Executives**



543 **Potentially Infected Employees**



30
COMPANIES

SPANNING THESE INDUSTRY FIELDS

Engineering • Construction • Homebuilding



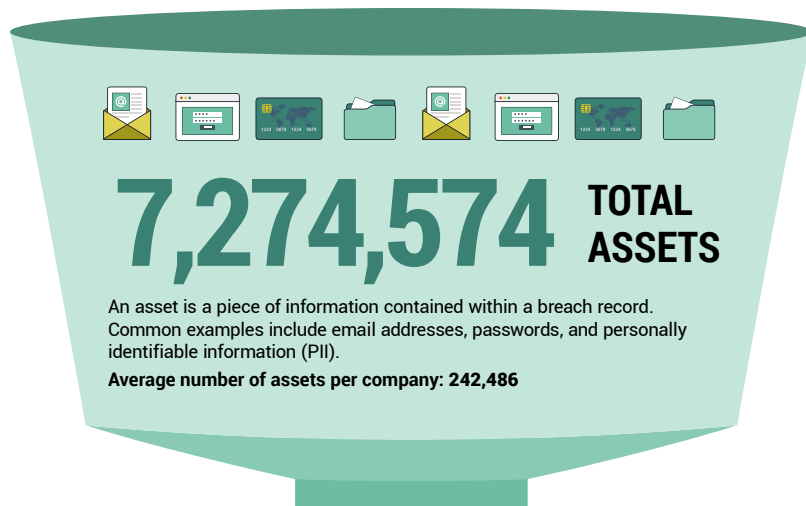
3,034 **TOTAL BREACH SOURCES**

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



1,423,785 **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: 47,460**



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.



3,901,644

TOTAL PII ASSETS

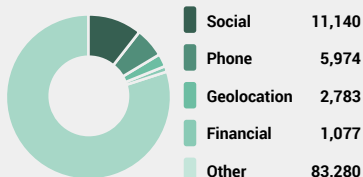
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 130,055



3,127,644 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



245,286

TOTAL CORPORATE EXPOSED CREDENTIALS

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

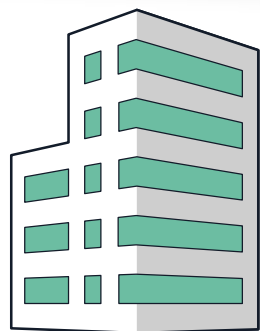


8,176 **Average Number of Exposed Passwords per Company**

3,103 **Potentially Exposed C-Level Executives**



332 **Potentially Infected Employees**



162
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)



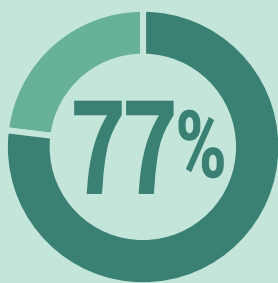
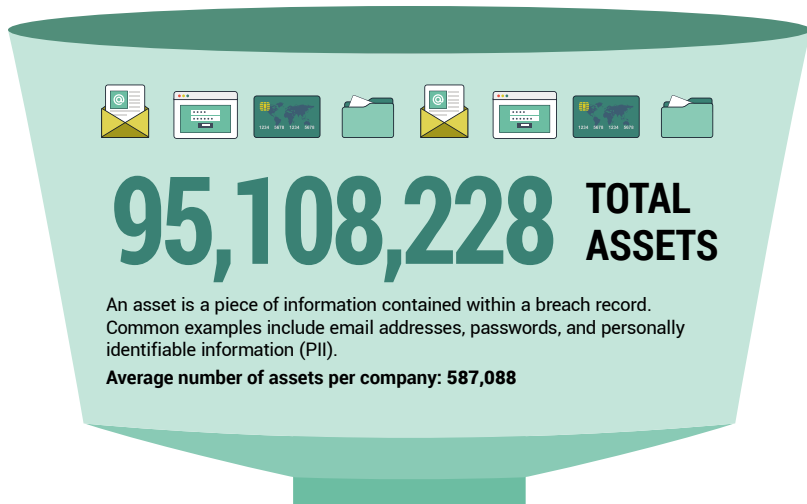
7,790 **TOTAL BREACH SOURCES**

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



18,085,495 **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: 111,639**



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.



51,364,748

TOTAL PII ASSETS

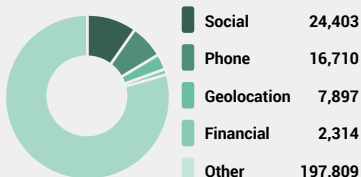
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 317,066



40,359,532 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



3,383,948

TOTAL CORPORATE EXPOSED CREDENTIALS

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

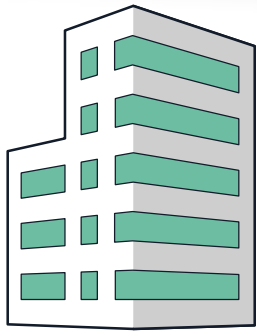


20,889 **Average Number of Exposed Passwords per Company**

39,328 **Potentially Exposed C-Level Executives**



1,646 **Potentially Infected Employees**



10
COMPANIES

SPANNING THESE INDUSTRY FIELDS
Grocery and Food Stores • Pharmacy and Drug Stores



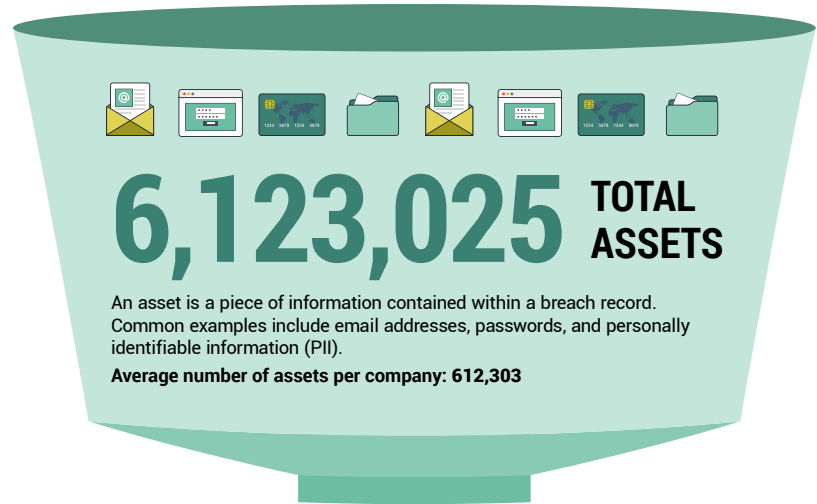
1,007 **TOTAL BREACH SOURCES**

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



923,297 **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: 92,330**



6,123,025 **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: 612,303



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.



3,742,928

TOTAL PII ASSETS

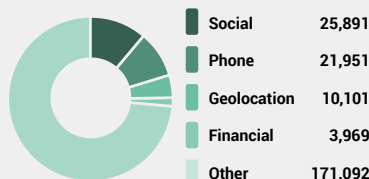
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 374,293



2,330,045 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



50,052

TOTAL CORPORATE EXPOSED CREDENTIALS

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

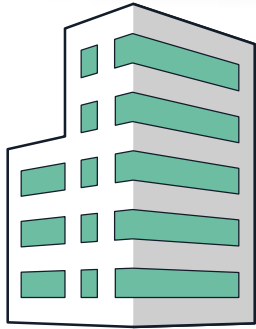


5,005 **Average Number of Exposed Passwords per Company**

1,062 **Potentially Exposed C-Level Executives**



98 **Potentially Infected Employees**



37
COMPANIES

SPANNING THESE INDUSTRY FIELDS

Beverage Products

Food Production

Food Consumer Products

Tobacco Products



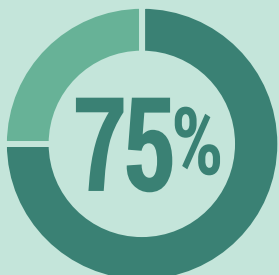
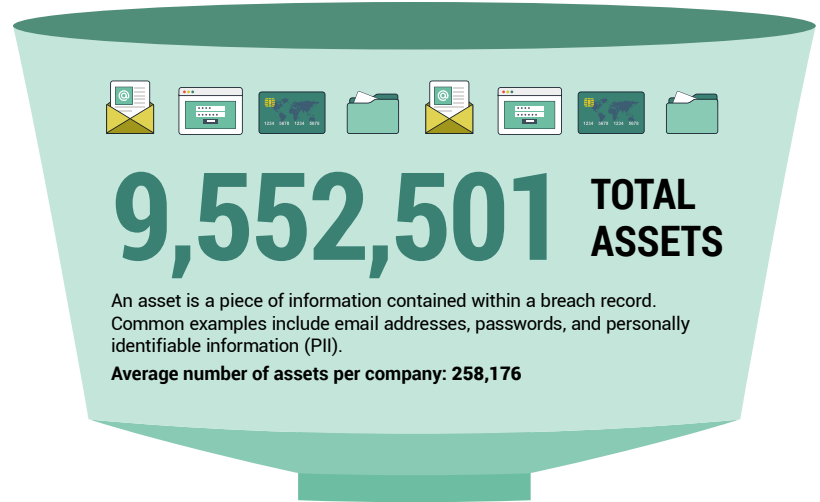
3,885 TOTAL BREACH SOURCES

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



1,684,564 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: 45,529**



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.



5,353,931

TOTAL PII ASSETS

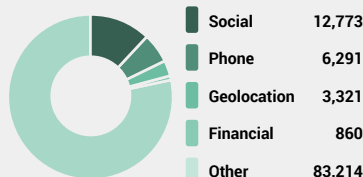
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 144,701



3,938,982 TOTAL OTHER ASSETS

Average Other Assets Per Company



259,588 TOTAL CORPORATE EXPOSED CREDENTIALS

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

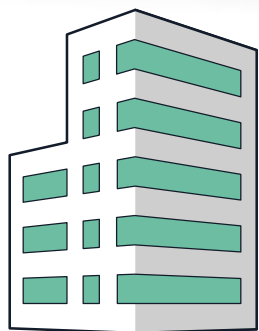


7,016 Average Number of Exposed Passwords per Company

2,644 Potentially Exposed C-Level Executives



445 Potentially Infected Employees



71
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



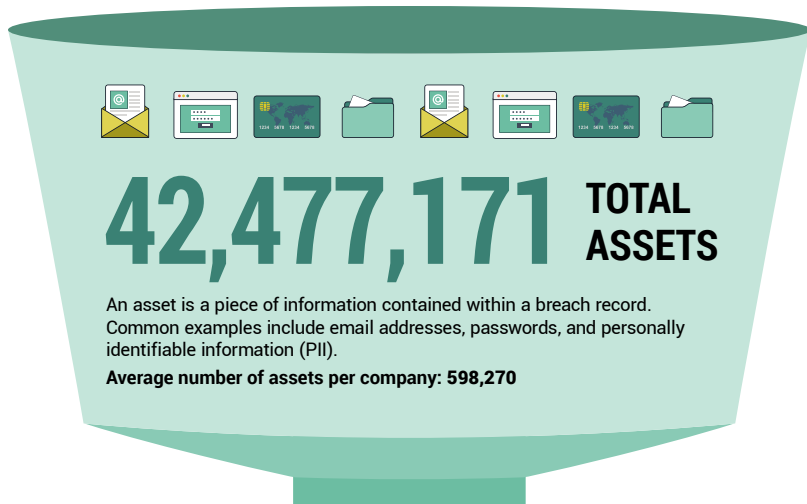
6,957 **TOTAL BREACH SOURCES**

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



7,809,751 **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: 109,996**



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.



23,015,611

TOTAL PII ASSETS

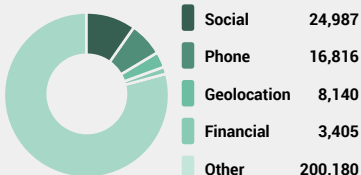
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 324,164



18,000,490 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



1,461,070

TOTAL CORPORATE EXPOSED CREDENTIALS

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

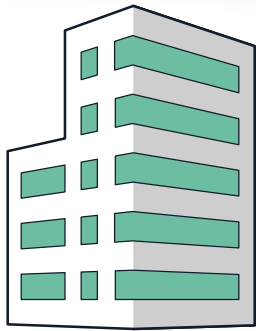


20,578 **Average Number of Exposed Passwords per Company**

9,789 **Potentially Exposed C-Level Executives**



1,120 **Potentially Infected Employees**



27

COMPANIES

SPANNING THESE INDUSTRY FIELDS

Food Services • Hotels, Casinos & Resorts



3,354

TOTAL BREACH SOURCES

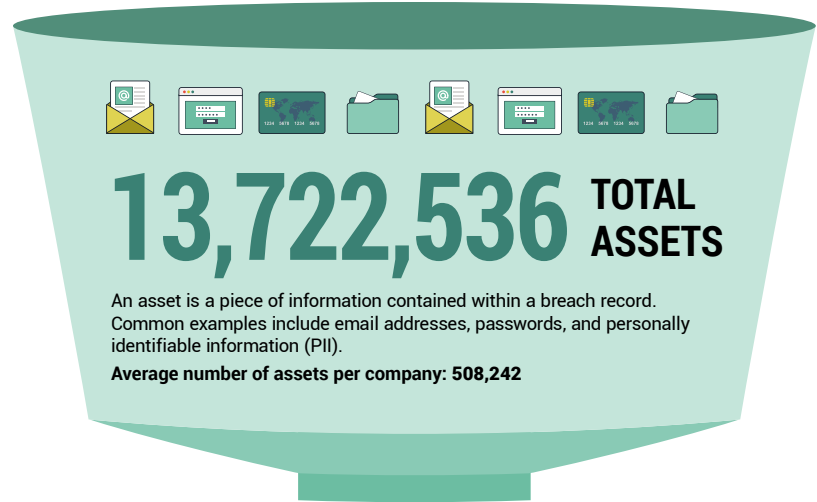
The number of breaches within the SpyCloud database that include records tied to Fortune 1000 corporate email addresses in this sector.



2,448,465

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: 90,684**

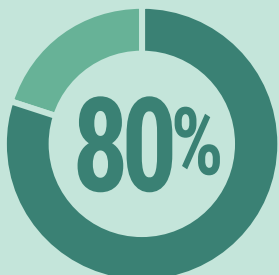


13,722,536

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: 508,242



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.



7,748,981

TOTAL PII ASSETS

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

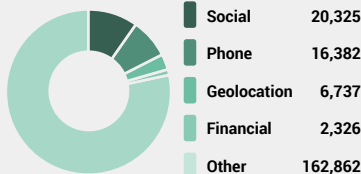
Average PII Assets per Company: 286,999



5,633,055

TOTAL OTHER ASSETS

Average Other Assets Per Company



340,500

TOTAL CORPORATE EXPOSED CREDENTIALS

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



12,611

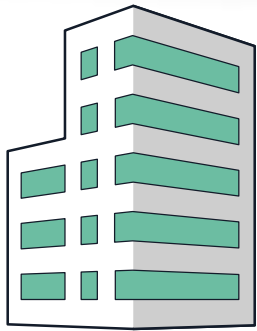
Average Number of Exposed Passwords per Company

8,639

Potentially Exposed C-Level Executives

450

Potentially Infected Employees



26
COMPANIES

SPANNING THESE INDUSTRY FIELDS

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



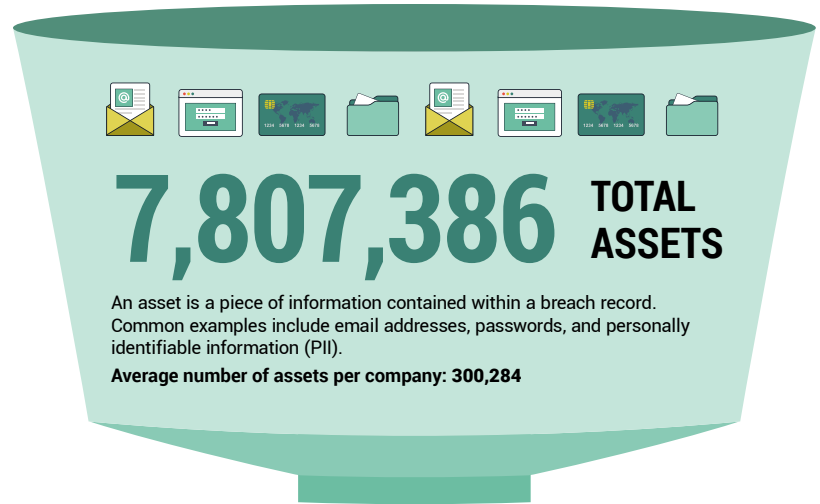
4,248 TOTAL BREACH SOURCES

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



1,463,594 TOTAL BREACH RECORDS

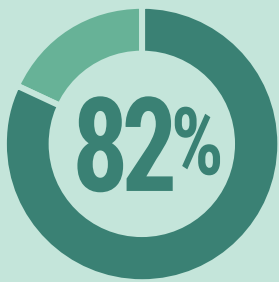
A breach record is the set of data tied to a single user within a given breach. One employee whose information appears in three different breaches would result in three distinct breach records. Each record may contain a different set of assets. **Average number of breach records per company in this sector: 56,292**



7,807,386 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: 300,284



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.



4,113,668

TOTAL PII ASSETS

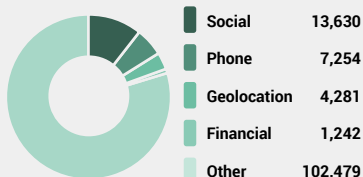
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 158,218



3,351,019 TOTAL OTHER ASSETS

Average Other Assets Per Company



342,699

TOTAL CORPORATE EXPOSED CREDENTIALS

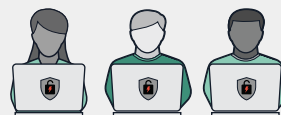
Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.



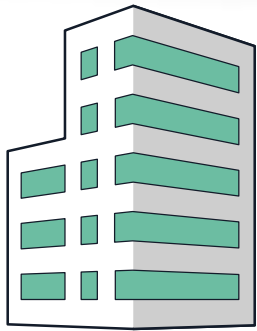
13,181

Average Number of Exposed Passwords per Company

2,554 Potentially Exposed C-Level Executives



319 Potentially Infected Employees



50
COMPANIES

SPANNING THESE INDUSTRY FIELDS

Construction and Farm Machinery Industrial Machinery
Electronics, Electrical Equipment Miscellaneous



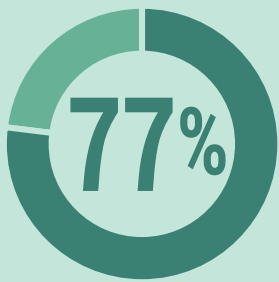
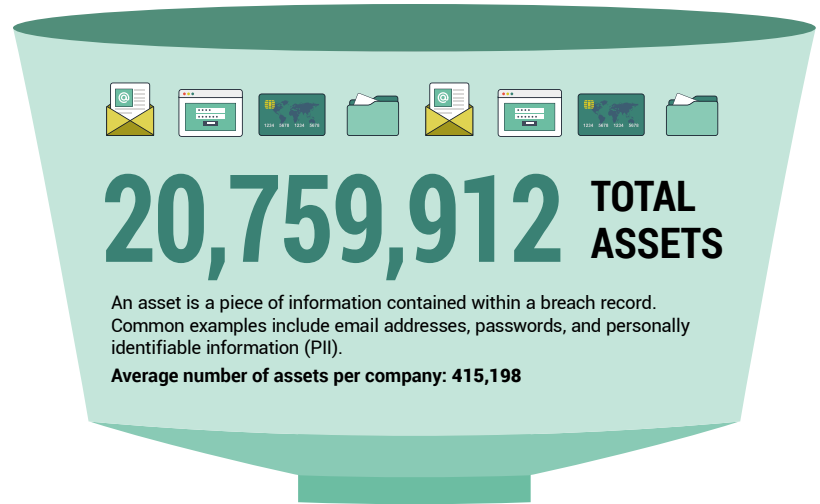
7,315 **TOTAL BREACH SOURCES**

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



4,356,468 **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: 87,129**



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.



10,248,472

TOTAL PII ASSETS

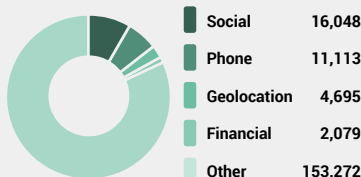
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 204,969



9,360,322 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



1,151,118

TOTAL CORPORATE EXPOSED CREDENTIALS

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



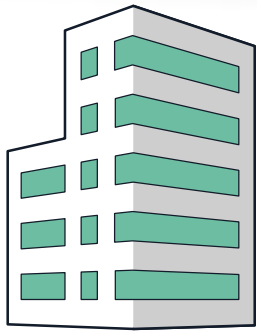
23,022 **Average Number of Exposed Passwords per Company**

5,329

Potentially Exposed C-Level Executives



1,018 **Potentially Infected Employees**



46
COMPANIES

SPANNING THESE INDUSTRY FIELDS

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



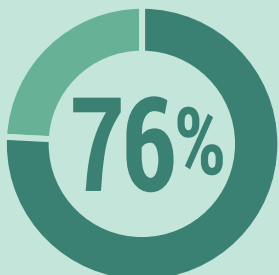
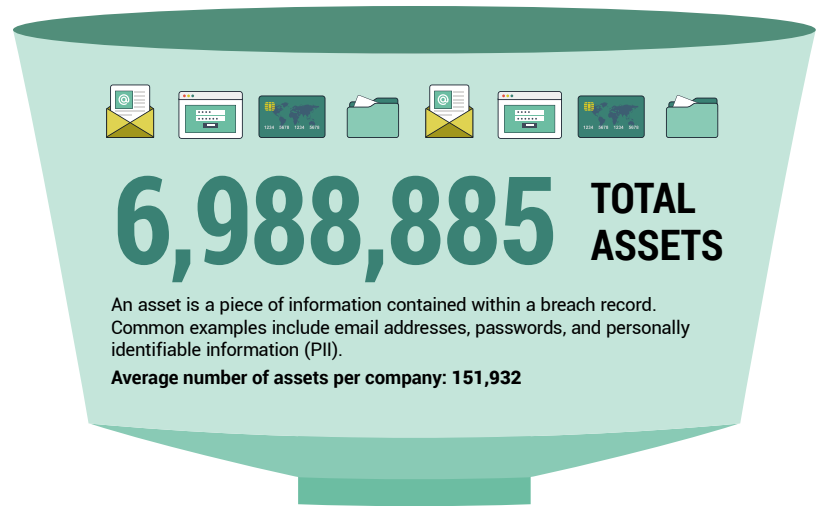
3,255 **TOTAL BREACH SOURCES**

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



1,305,926 **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: 28,390**



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.



3,789,600

TOTAL PII ASSETS

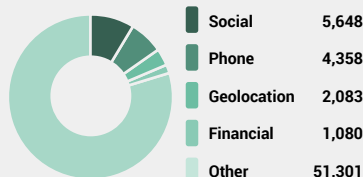
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 82,383



2,965,594 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



233,691

TOTAL CORPORATE EXPOSED CREDENTIALS

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

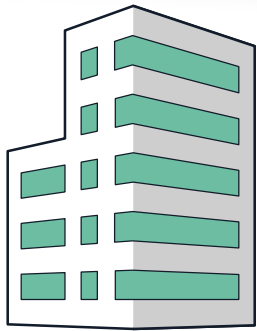


5,080 **Average Number of Exposed Passwords per Company**

2,395 **Potentially Exposed C-Level Executives**



202 **Potentially Infected Employees**



25
COMPANIES

SPANNING THESE MEDIA FIELDS
Entertainment • Publishing • Printing



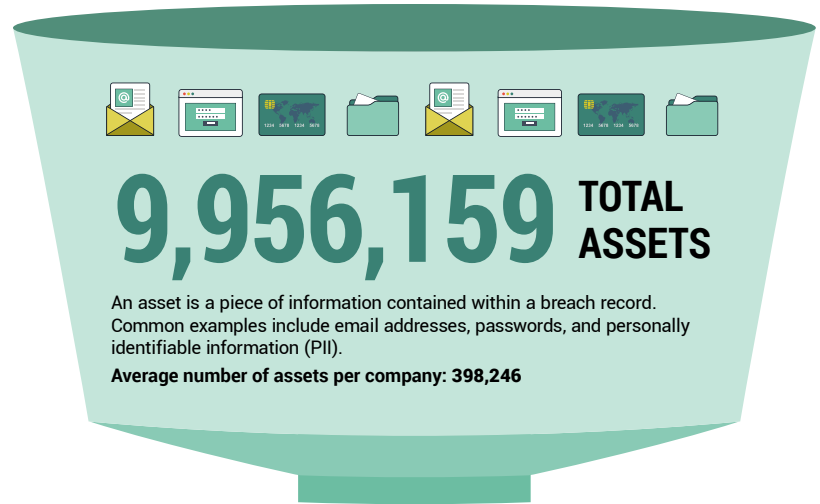
4,155 **TOTAL BREACH SOURCES**

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



2,474,905 **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: 98,996**



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.



3,664,535

TOTAL PII ASSETS

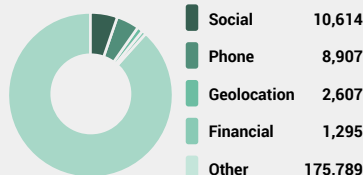
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 146,581



4,980,329 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



1,311,295 **TOTAL CORPORATE EXPOSED CREDENTIALS**

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

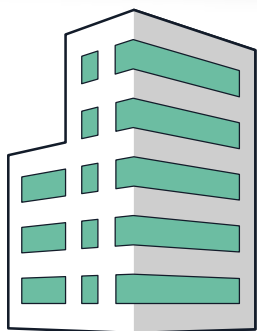


52,452 **Average Number of Exposed Passwords per Company**

2,194 **Potentially Exposed C-Level Executives**



1,046 **Potentially Infected Employees**



22
COMPANIES

FROM MOTOR VEHICLES & PARTS



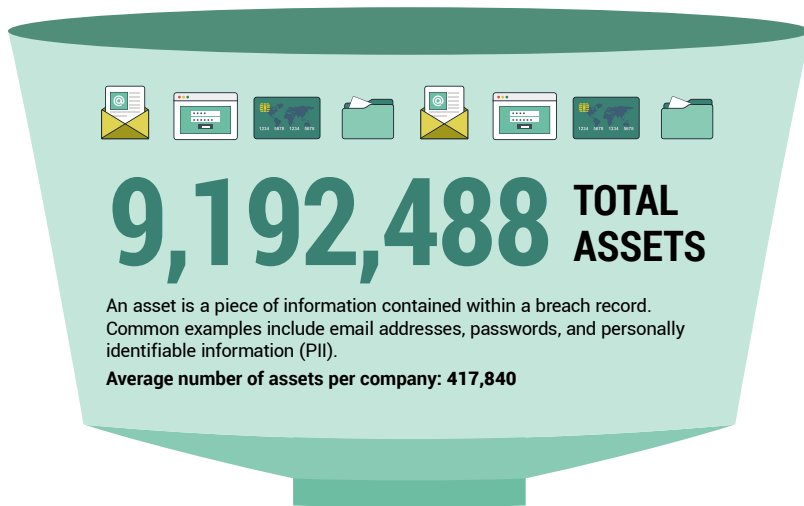
4,688 TOTAL BREACH SOURCES

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



1,611,017 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: 73,228**



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.



4,883,081

TOTAL PII ASSETS

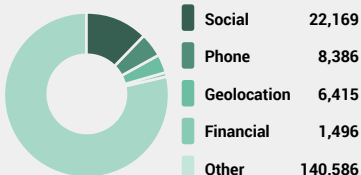
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 221,958



3,939,145 TOTAL OTHER ASSETS

Average Other Assets Per Company



370,262

TOTAL CORPORATE EXPOSED CREDENTIALS

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

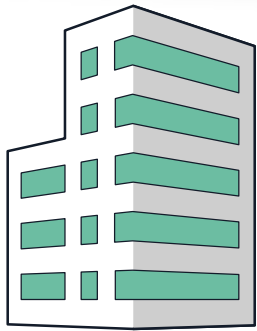


16,830 Average Number of Exposed Passwords per Company

2,091 Potentially Exposed C-Level Executives



632 Potentially Infected Employees



75
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



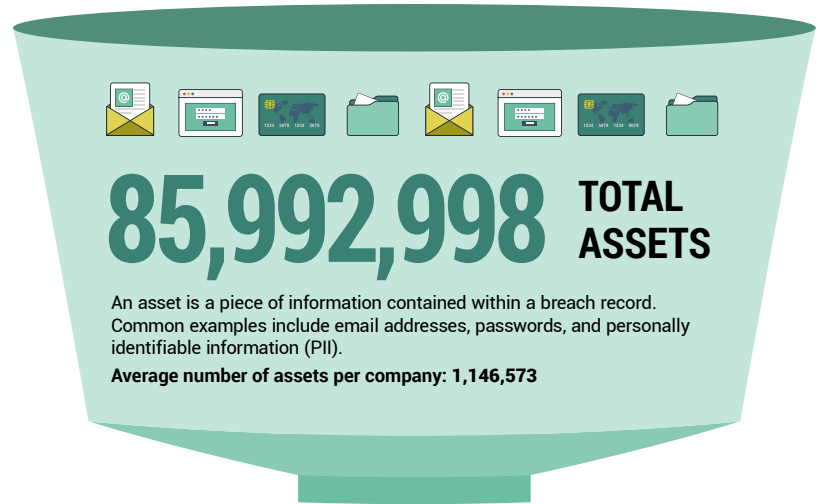
4,372 **TOTAL BREACH SOURCES**

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



14,366,328 **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: 191,551**



85,992,998 **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: 1,146,573



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.



54,047,920

TOTAL PII ASSETS

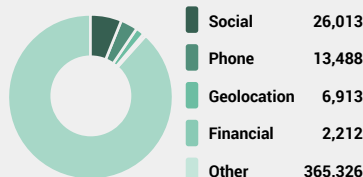
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 720,639



31,046,416 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



898,662

TOTAL CORPORATE EXPOSED CREDENTIALS

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

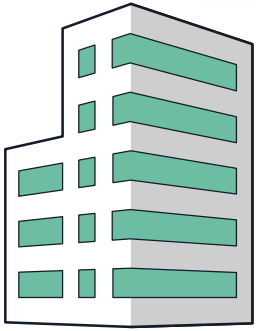


11,982 **Average Number of Exposed Passwords per Company**

11,707 **Potentially Exposed C-Level Executives**



1,652 **Potentially Infected Employees**



109
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



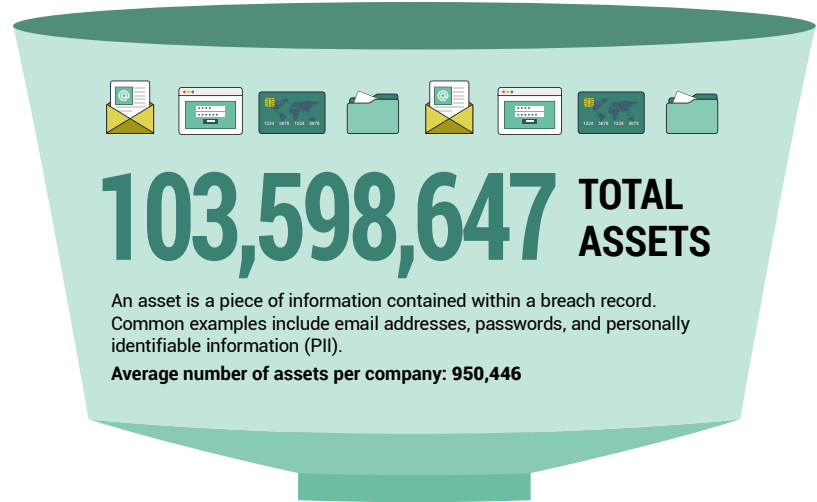
13,239 **TOTAL BREACH SOURCES**

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



22,130,723 **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: 203,034**



103,598,647 **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: 950,446



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.



47,631,316

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: 436,985



6,730,415

TOTAL CORPORATE EXPOSED CREDENTIALS

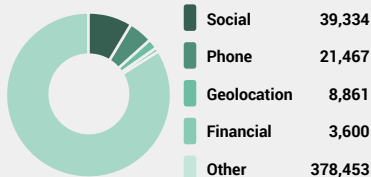
Corporate credentials include pairings of corporate email addresses and plaintext (cracked) passwords that are fully exploitable and ready for criminals to use.



61,747 **Average Number of Exposed Passwords per Company**

49,236,916 **TOTAL OTHER ASSETS**

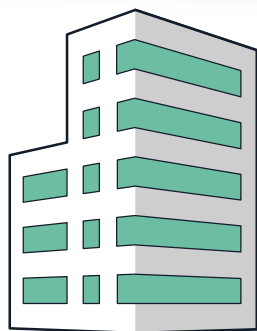
Average Other Assets Per Company



16,399 **Potentially Exposed C-Level Executives**



13,897 **Potentially Infected Employees**



11
COMPANIES

FROM THE TELECOM INDUSTRY



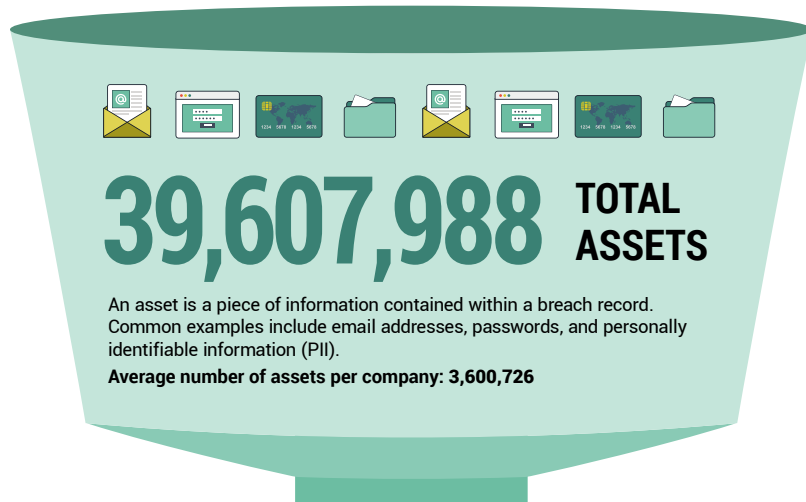
6,507 **TOTAL BREACH SOURCES**

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



11,294,240 **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: 1,026,749**



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.



11,755,682

TOTAL PII ASSETS

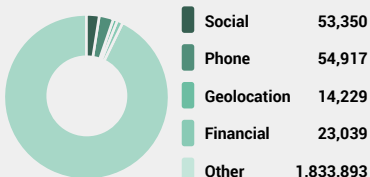
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 1,068,698



21,773,699 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



6,078,607

TOTAL CORPORATE EXPOSED CREDENTIALS

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

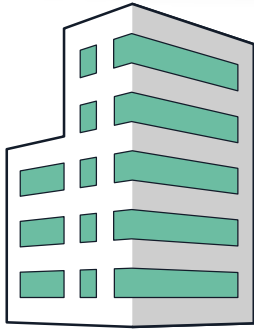


552,601 **Average Number of Exposed Passwords per Company**

2,399 **Potentially Exposed C-Level Executives**



2,328 **Potentially Infected Employees**



38
COMPANIES

SPANNING THESE TRANSPORT FIELDS

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



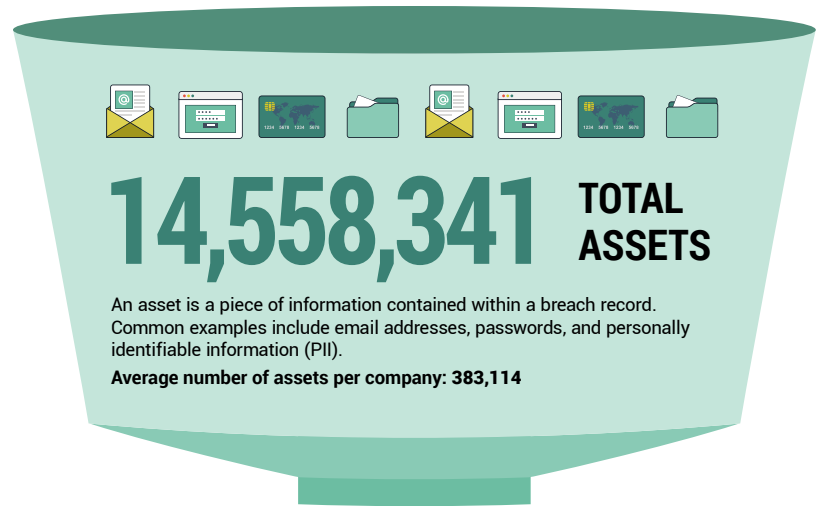
4,761 **TOTAL BREACH SOURCES**

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



2,843,305 **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: 74,824**



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.



7,742,690

TOTAL PII ASSETS

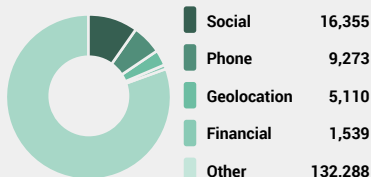
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 203,755



6,253,450 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



562,201

TOTAL CORPORATE EXPOSED CREDENTIALS

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

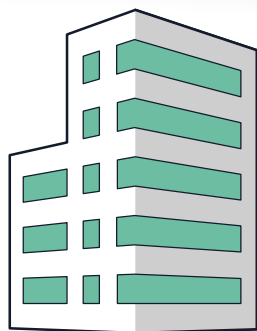


14,795 **Average Number of Exposed Passwords per Company**

4,540 **Potentially Exposed C-Level Executives**



683 **Potentially Infected Employees**



35
COMPANIES

SPANNING THESE WHOLESALE FIELDS

- Wholesalers: Diversified
- Wholesalers: Electronics and Office Equipment
- Wholesalers: Food and Grocery



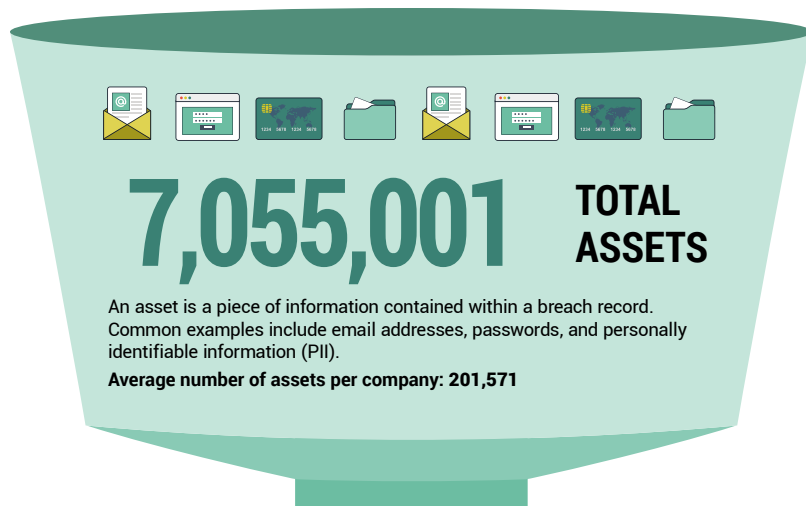
2,783 **TOTAL BREACH SOURCES**

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



1,345,519 **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: 38,443**



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.



3,838,200

TOTAL PII ASSETS

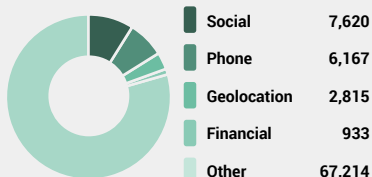
Personally identifiable information (PII) may include data such as addresses, social security info, credit ratings, and more.

Average PII Assets per Company: 109,663



2,966,179 **TOTAL OTHER ASSETS**

Average Other Assets Per Company



250,622 **TOTAL CORPORATE EXPOSED CREDENTIALS**

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



7,161 **Average Number of Exposed Passwords per Company**

2,999 **Potentially Exposed C-Level Executives**



235 **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 543 million breach assets in criminals' hands, 25.9 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.

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.



Employee ATO Prevention

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

[Learn More →](#)



VIP Guardian

Protect your highest-risk executives from targeted account takeover.

[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 →](#)



Consumer ATO Prevention

Protect your users from account takeover fraud and unauthorized purchases.

[Learn More →](#)

[See Your Account Takeover Risk →](#)

Discover how many breach records we have associated with your email address and your domain as a whole. Once you know, you can take action.