Constella

Financial Services Sector Exposure Report

2018-2021 Digital Risk Findings and Trends

Introduction

Following the release of Constella Intelligence's 2021 Identity Breach Report, new and additional findings pertaining to exposures, breaches, and leakages within the financial services (Finserv) sector, specifically focusing on employees and executives from the top twenty Finserv companies on the Fortune Global 500 list, have been compiled in this industry-specific report which examines data from January 2018 through September 2021.

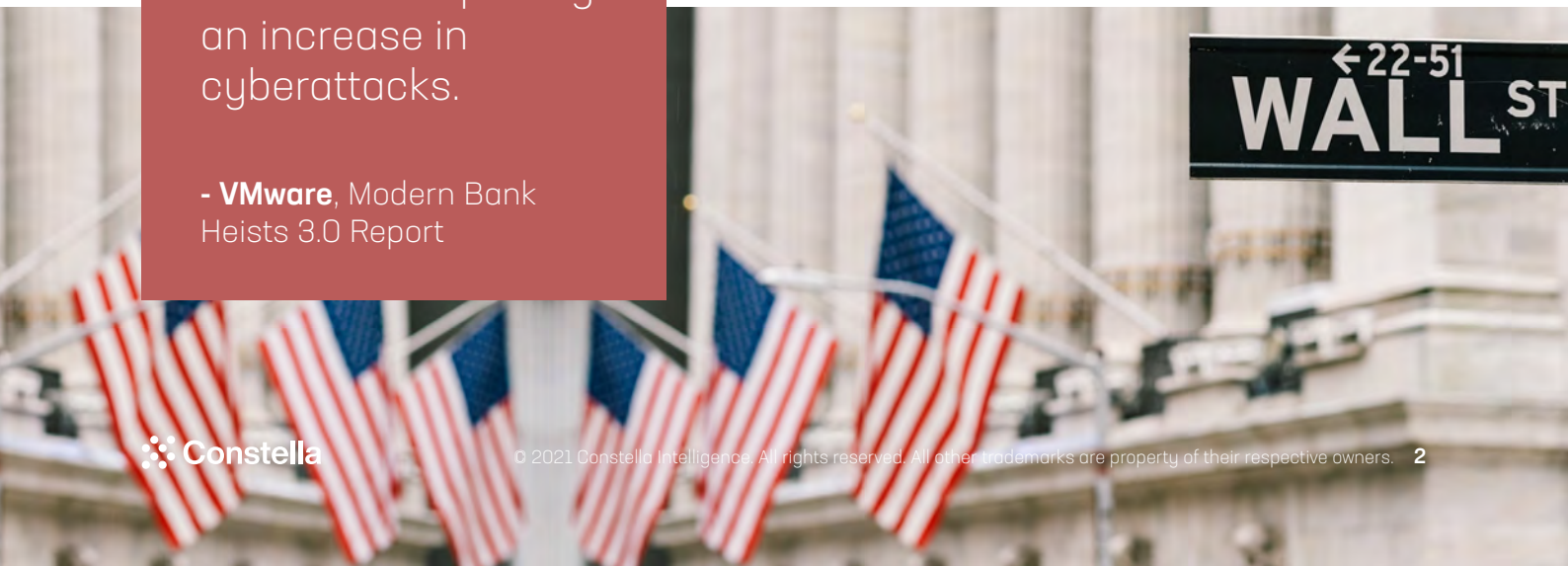
Financial institutions are entrusted with an individual's most sensitive and personally identifiable information making them high-value targets for cyber threat actors. They also have an added layer of fiduciary responsibility to safeguard these assets, driven by regulatory requirements from the FCRA, FTC, and others. These institutions have access to social security numbers, credit card information, bank account numbers, email addresses, and passwords. These assets can be exploited to inflict severe economic damage on an exposed individual and the financial institution. A breach can also impact the reputation of the financial institution. For financial institutions, trust is paramount, and the public nature of a data breach can cripple reputations and undermine consumer confidence.

Cyber attacks on businesses in the Finserv sector are the most costly of all, resulting in an average of $18.3 million in losses annually per company, according to data published by Accenture. Attacks continue to surge because banks hold sensitive, high-value data. During the Covid-19 pandemic, this has only intensified.

Recently Morgan Stanley, a leading global investment bank and wealth management firm, disclosed that the personal data of some of its corporate clients was stolen in a data breach that involved a third-party vendor. Hackers accessed sensitive information, including social security numbers, addresses, and the date of birth of its most important clients.

> According to cybersecurity firm VMware, attacks against the financial sector increased 238% globally from February to April 2020, with some 80% of financial institutions reporting an increase in cyberattacks.
>
> **- VMware**, Modern Bank Heists 3.0 Report

And it's only getting worse. Cyberattacks against the Finserv sector will continue since the financial gain is so attractive to hackers, leaving a bullseye on the backs of financial institutions – reaffirming the need for organizations to adopt comprehensive digital risk protection practices for executives, key employees and trusted vendors who have access to critical systems and sensitive data. As experts in digital risk protection, cyber intelligence, and cybersecurity continue to track and anticipate cybercrime activity targeting the industry, it is essential to raise awareness regarding the principal points of attack from threat actors and the vulnerabilities often exploited through employees, vendors and executives. This report explores the ongoing digital threats plaguing the Finserv sector and highlights the prevalence of exposures related to the corporate credentials of executives and employees.

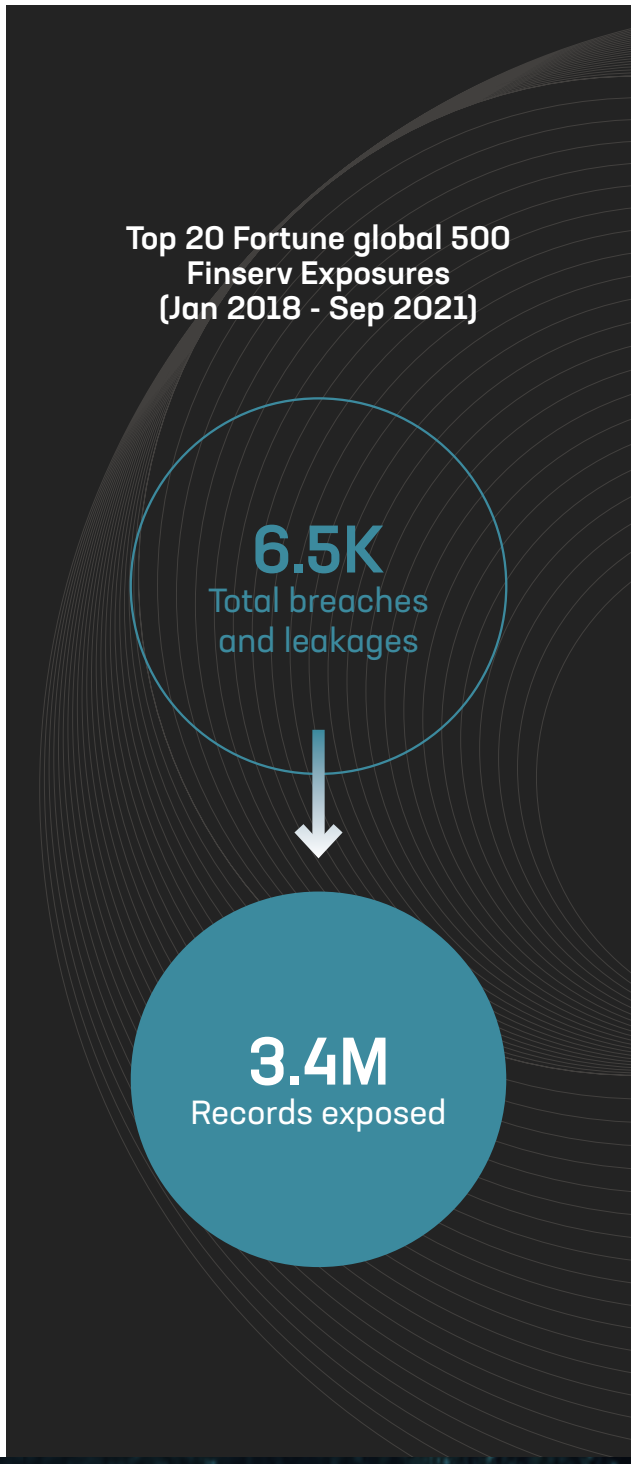


Executive Summary

The rapid digital transformation of organizations in the Finserv sector has dramatically expanded attack surfaces. This means that these companies, their executives, and their key employees are high-value targets for cybercriminals and threat actors. Given the critical services offered by companies operating in this space and the sensitivity of data relevant to consumers in this sector, Constella Intelligence conducted an analysis of metrics pertaining to the digital vulnerabilities of major Finserv organizations. This analysis was conducted by aggregating and analyzing exposures of the top twenty financial services companies on the Fortune Global 500 list, including a sample of executives from these companies. Constella's analysis assessed exposures from 2018 to 2021. The results of the analysis demonstrate a progressive increase in exposures of records through a growing number of breaches year over year.

From January 2018 to September 2021, Constella Intelligence's threat intelligence team, using identity records from data breaches and leakages found in open sources, on social media, and the surface deep and dark web, identified **6,472 breaches** and leakages and **3,367,059 exposed records** from the companies analyzed. These metrics are startling and reflect the gravity of digital vulnerabilities enabled by the billions of records of personally identifiable information (PII) available and transacted daily in the digital sphere.

Constella Intelligence's research indicates that in 2018, 2019, and 2020 the breach count was 1,320, 1,535, and 2,206, respectively. Over the same three-year period, the number of total identity records exposed also increased from 194,656 (2018) to 889,444 (2019), and then to 1,371,779 (2020) **a six-fold increase in just two years**. Moreover, breaches identified from January to September of 2021 account for over **one in five (22%) of all breaches since 2018**, and the number of records exposed in 2021 so far makes up **more than one in four (27%) of all exposures since 2018.**



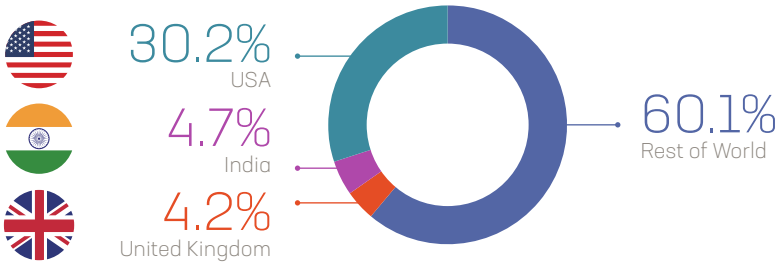
TWO-THIRDS OF BREACHES AND LEAKAGES IN THE FINANCIAL SERVICES SECTOR INCLUDE PII

Approximately two-thirds (66%) of the breaches and leakages identified include PII. Among the most common attributes were email, password, name, username, phone number, address, date of birth, and credit card information.

Among the breaches and leakages analyzed, Constella Intelligence focused on exposures of a sample of executives from the companies analyzed. In reviewing exposures of 79 executives from the top twenty Finserv companies, the team found that the corporate credentials of seven in ten (71%) of these executives have been exposed in a breach since 2018.

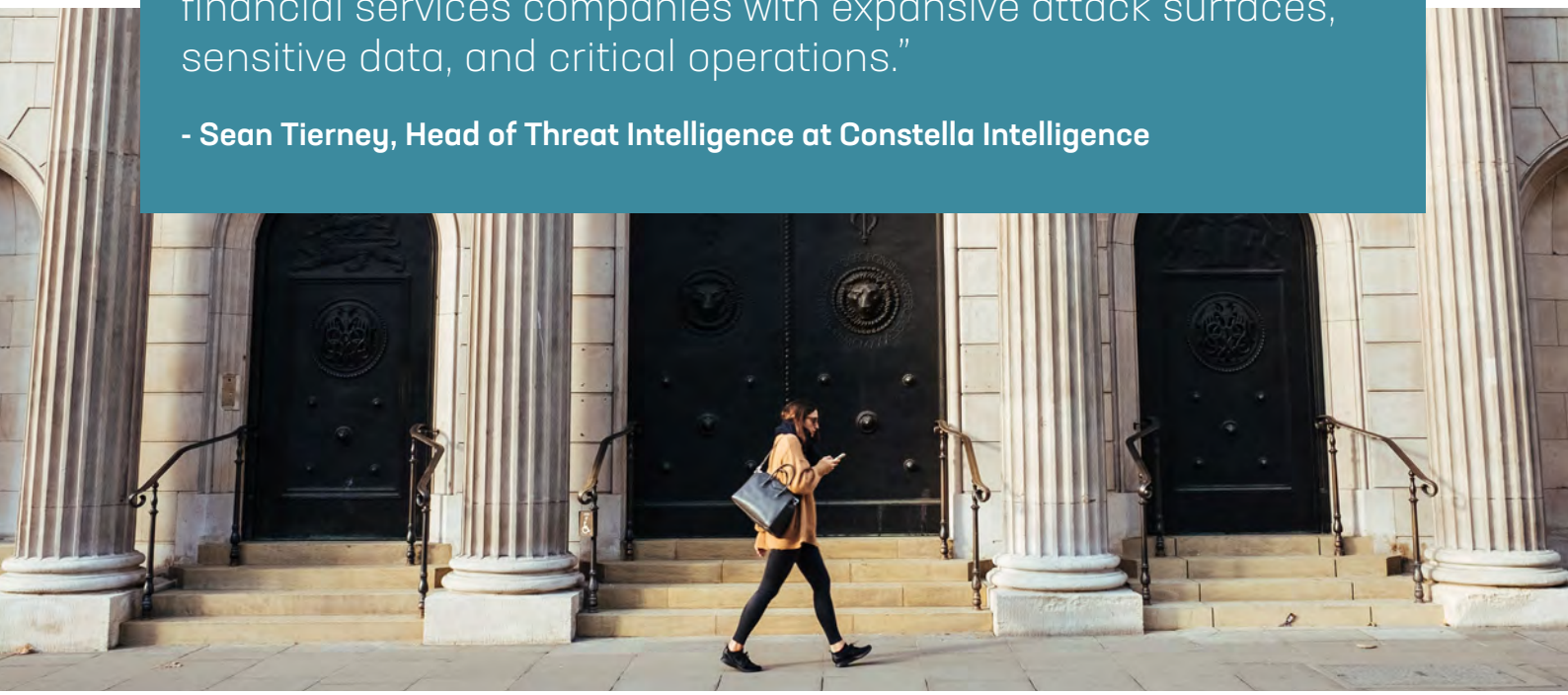
Constella Intelligence's Financial Services Sector Exposure Report offers insights into the cyber threats against the world's largest Finserv companies and their executives, underlining the proliferation of exposed personal records and corporate credentials. Left unchecked, this exposed data spells serious digital risk for global companies with expansive attack surfaces, sensitive data, and critical operations.

FINANCIAL SECTOR CREDENTIAL EXPOSURES - BY COUNTRY

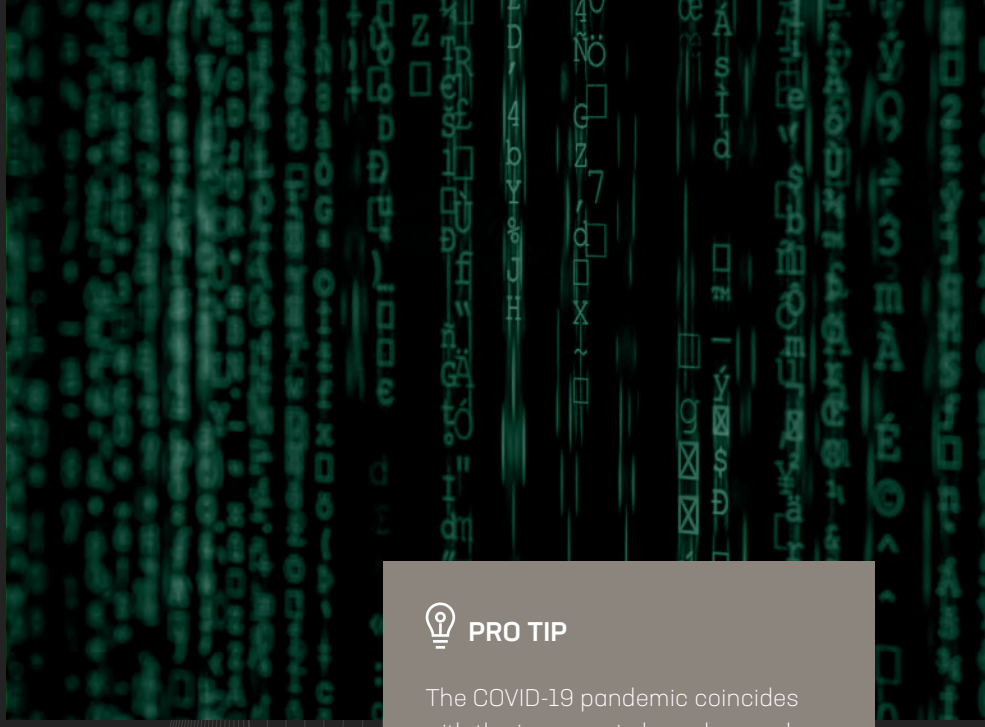


"Left unchecked, this exposed data spells serious digital risk for financial services companies with expansive attack surfaces, sensitive data, and critical operations."

- Sean Tierney, Head of Threat Intelligence at Constella Intelligence



Key Finding 1



Constella Intelligence's analysis identified over 3.3M exposed records from nearly 6.5K breaches and leakages between 2018 and 2021 where corporate credentials of major financial services companies were identified.

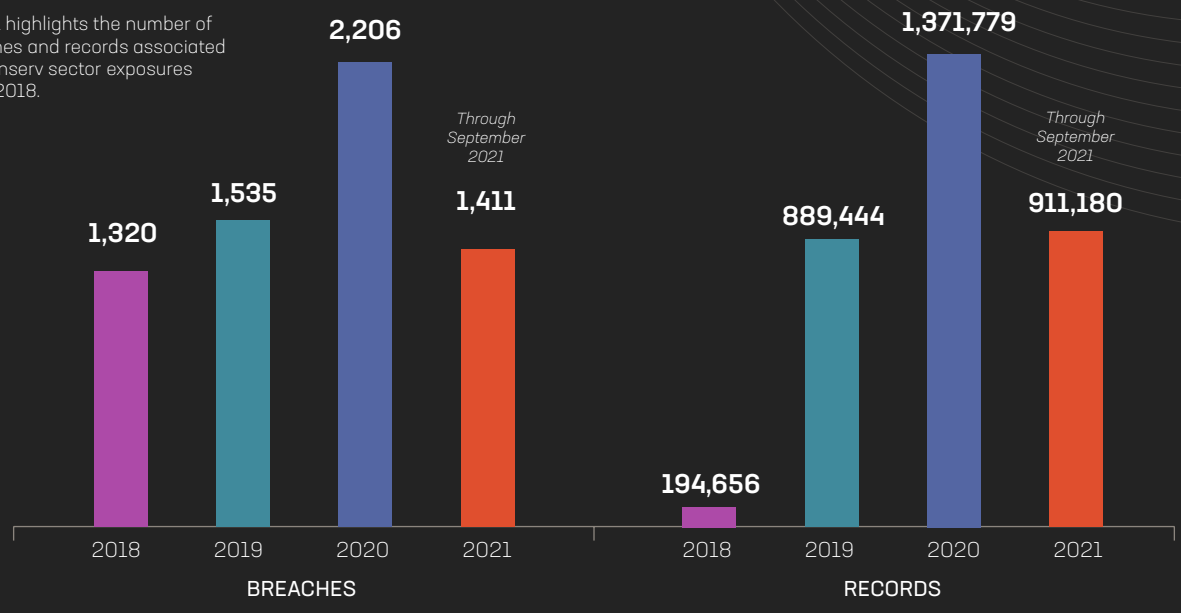
The analysis demonstrates a continuous increase in the number of breaches and the volume of records exposed for the top twenty Finserv companies since 2018. Moreover, around 22% of total breaches and 27% of total exposed records identified since 2018 occurred in the first nine months of 2021.

PRO TIP

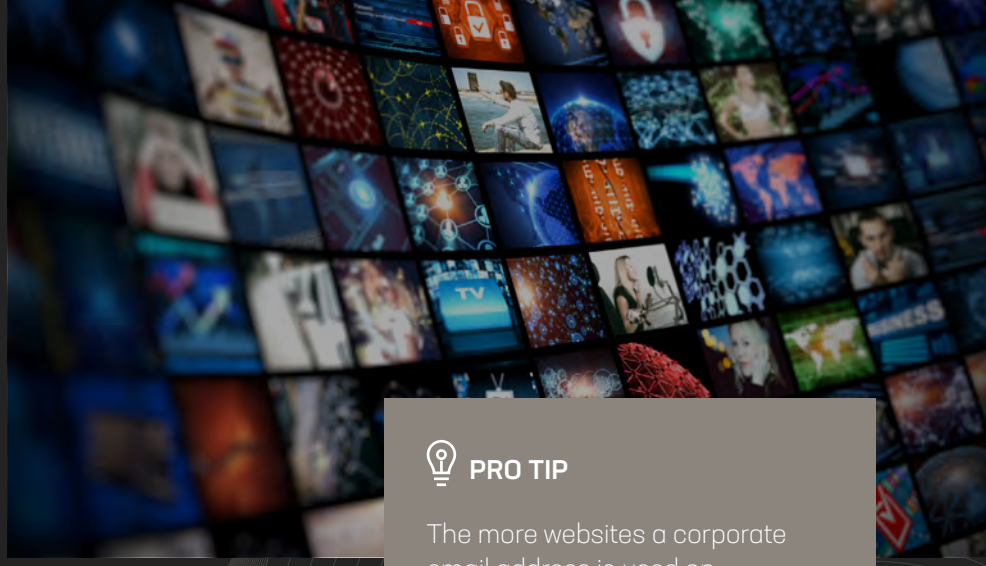
The COVID-19 pandemic coincides with the increase in breaches and records exposed in 2020 and 2021. With the move to hybrid and remote work models for many employees worldwide, company networks have seen increased vulnerabilities. For all organizations, it is important to ensure that proper security and password protocols are adhered to no matter where your employees are based, as threat actors aim to take advantage of the risks engendered by new hybrid work models.

TABLE 1. YEAR OVER YEAR BREACHES AND EXPOSED RECORDS

Table 1 highlights the number of breaches and records associated with Finserv sector exposures since 2018.



Key Finding 2



Finserv company employees incur severe digital risk to themselves and their company by using their corporate credentials on entertainment, news, retail, gaming, and other sites.

Domains where the corporate credentials of the Finserv companies analyzed have been exposed include entertainment, news, retail, gaming, and other technology and services sites. Usage of corporate credentials on these types of sites can indicate a lack of cyber hygiene and increases the attack surface of organizations, making employees a key vulnerability and attack vector.

PRO TIP

The more websites a corporate email address is used on, the more likely it is that an employee's information could be exposed. Poor corporate cyber hygiene, including the use of corporate emails on non-essential sites, can provide threat actors with better access to both the employee's work credentials and the company's systems. Keeping personal and professional accounts separate by using separate emails for each is an easy way to protect your employee credentials and company systems.

TABLE 2. SECTORS WHERE EMPLOYEE CREDENTIALS ARE EXPOSED

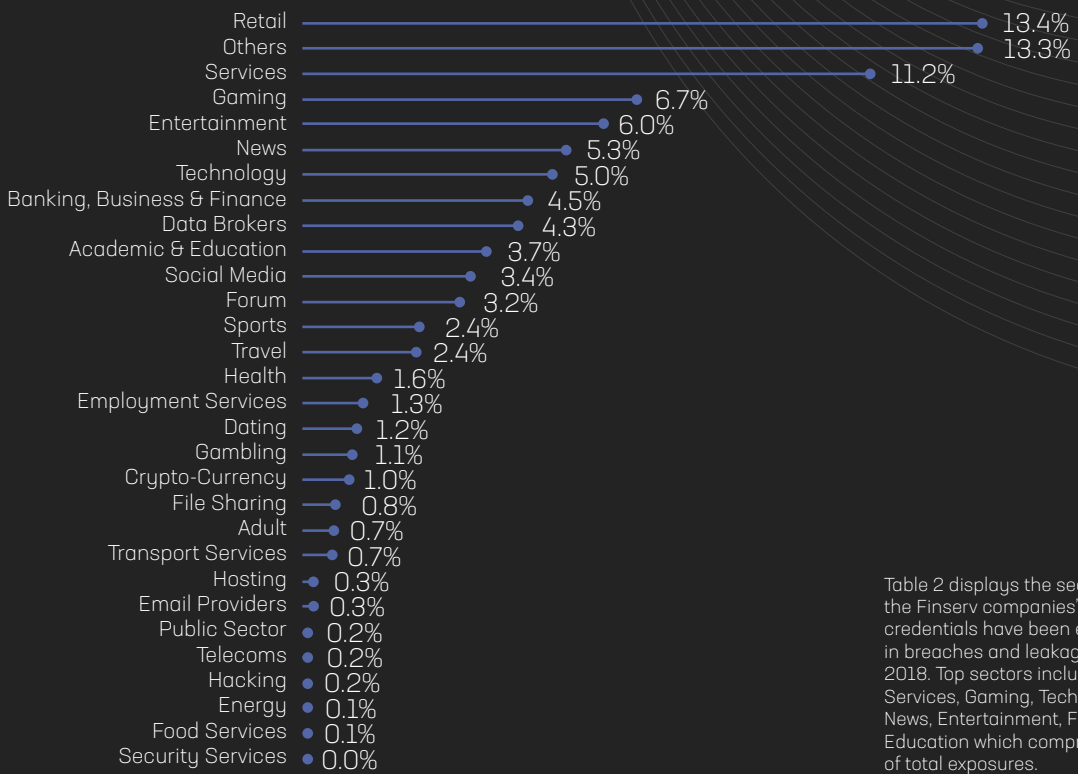
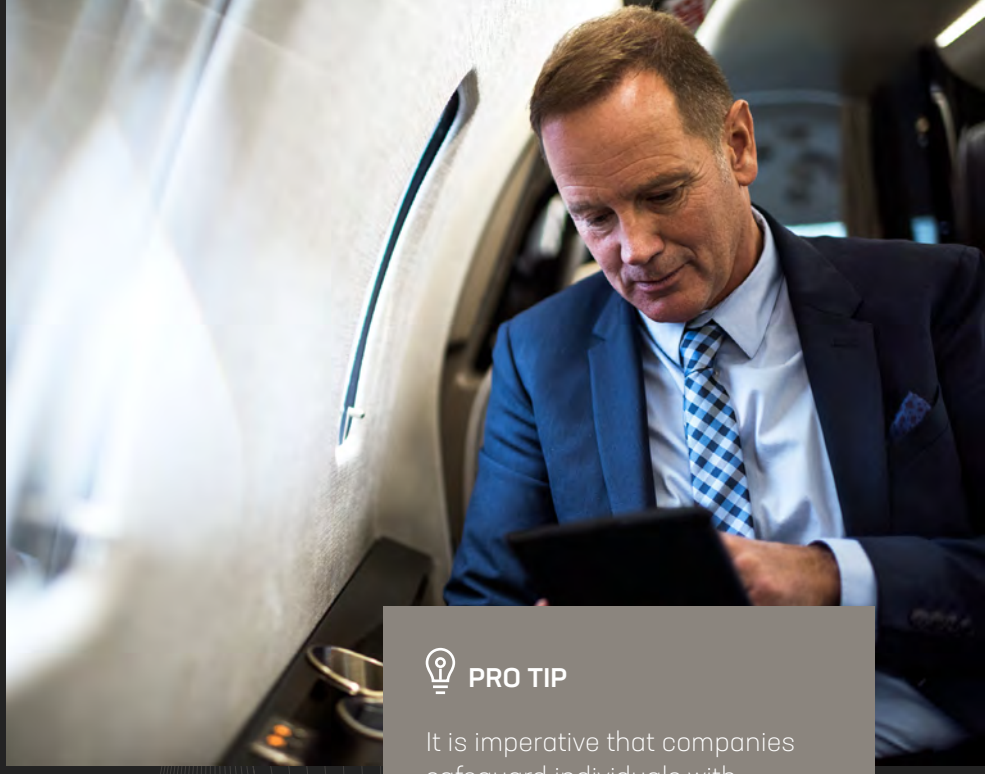


Table 2 displays the sectors where the Finserv companies' employee credentials have been exposed in breaches and leakages since 2018. Top sectors include Retail, Services, Gaming, Technology, News, Entertainment, Finance, and Education which comprise over 50% of total exposures.

Key Finding 3



Credential exposures and proliferation of the C-suite's PII are abundant, putting executives and their companies at greater risk of cyberattacks.

An analysis of a sample of 79 executives (C-suite profiles) from Fortune Global 500 Finserv companies, found that **71% of executives have had their corporate credentials exposed in a breach or leakage since 2018.** Of those 56 executives exposed, 55 (98%) have been exposed in breaches that include passwords.

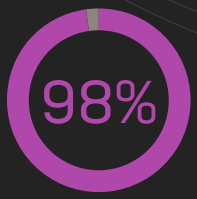
PRO TIP

It is imperative that companies safeguard individuals with privileged access to corporate networks and critical infrastructure. Constella Intelligence's analysis demonstrates the vast volume of sensitive employee and executive corporate credentials that are in circulation due to exposures and breaches. The more exposed personal data related to employees and executives that persists on social media, the surface, deep, and dark web, the higher the risk of attacks like ransomware, phishing, account takeover, CEO impersonations and others.

Out of a sample of 79 executives from Fortune 500 Finserv companies.

71% had their corporate credentials exposed in a breach or leakage since 2018.

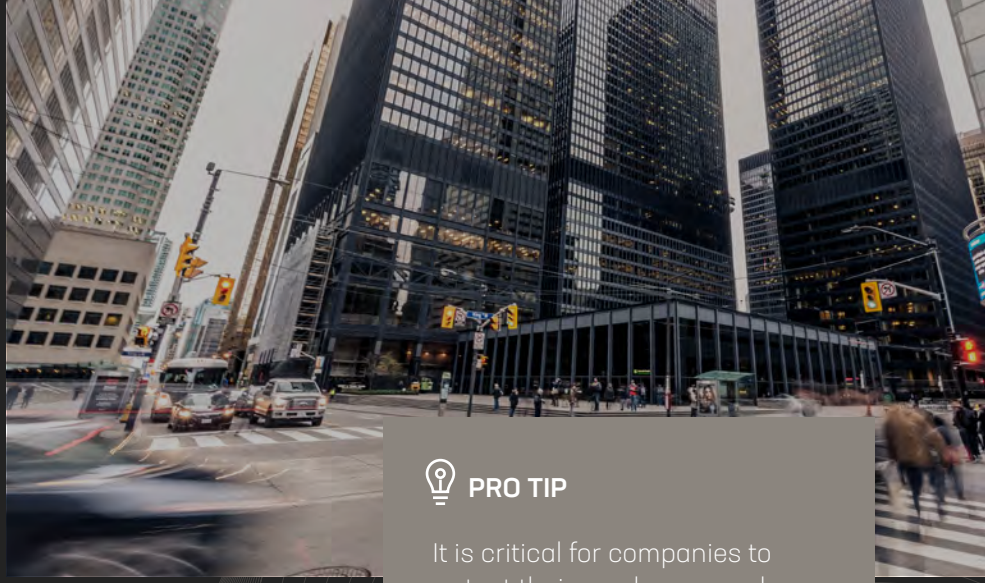
Of those exposed



98% have been exposed in breaches or leakages with PII.

2/5 have had their password exposed.

Key Finding 4



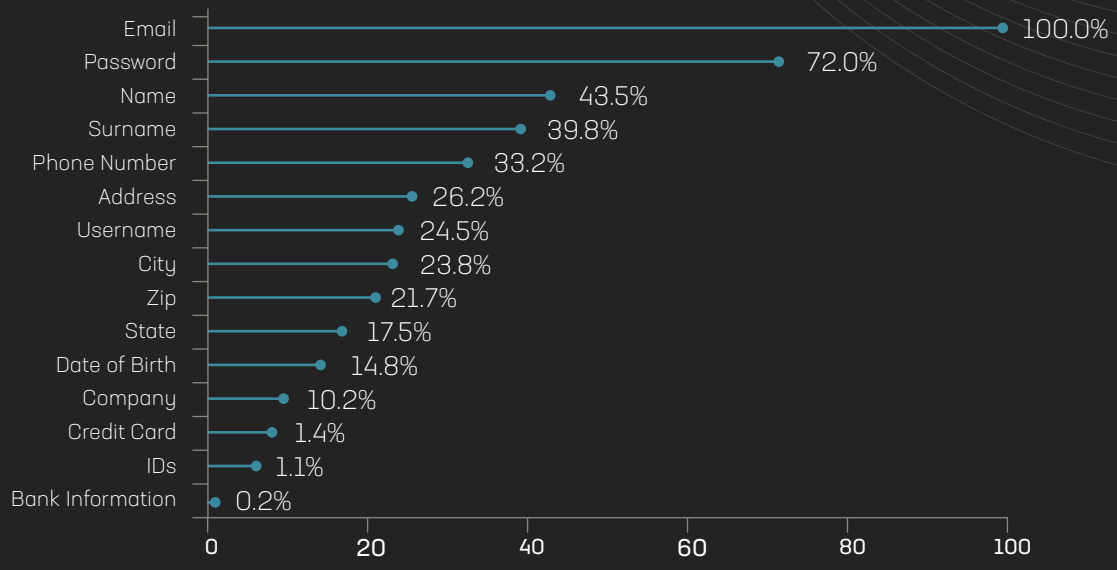
PRO TIP

It is critical for companies to protect their employees and for employees to recognize the implications of their personal information being exposed on the Internet. Changing passwords frequently, not reusing passwords, limiting sharing of personal information on public social platforms, applying customized privacy settings, and using multi-factor authentication are some of the ways employees can proactively protect their data.

Around two-thirds (66%) of Finserv sector breaches and leakages since 2018 include exposed PII, with the most common attributes being email (100%) and password (72%).

Exposed PII later sold or dumped in deep and dark marketplaces fuels the threat economy. With this data, cybercriminals can execute a wider range of sophisticated attacks targeting employees, executives, and brands including phishing, account take over, ransomware attacks, impersonation and coordinated disinformation campaigns. Emails appear in nearly 100% of breaches where Finserv employees have been exposed, while passwords appear more than 7 out of 10 breaches. Consistent with trends identified in Constella Intelligence's 2021 Identity Breach Report, 68% of passwords exposed are plaintext or are using a weak algorithm such as MD5 or SHA1.

TABLE 3. TOP FINSERV COMPANY ATTRIBUTES EXPOSED

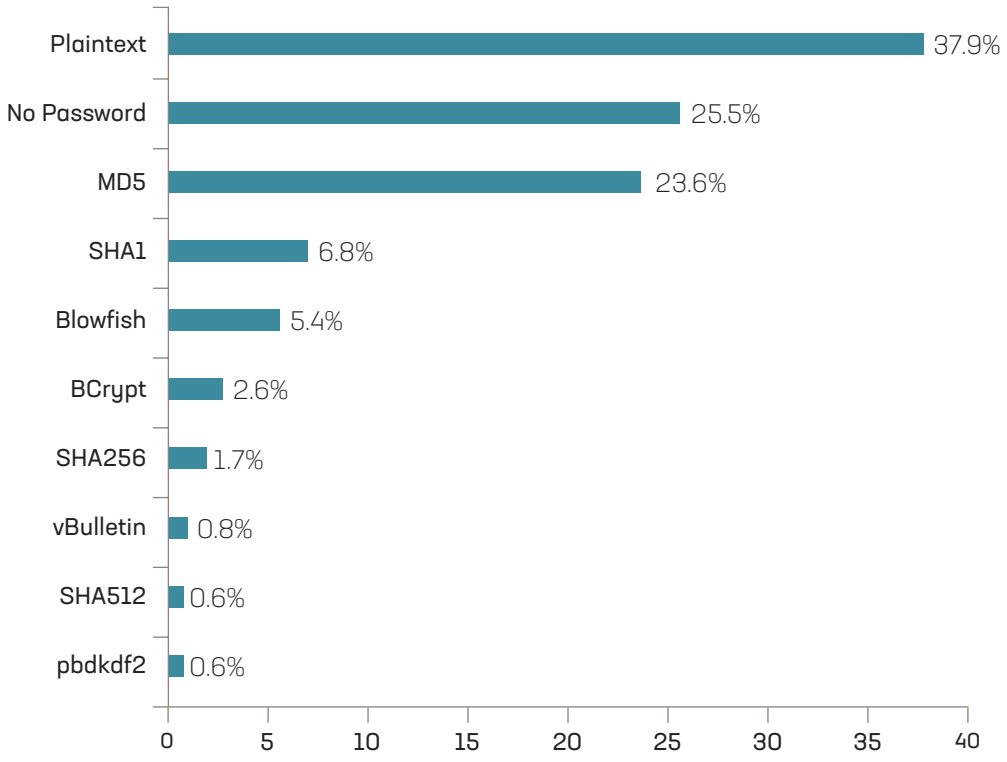


68%

of breaches between 2018 and 2021 are in plaintext, or use weak algorithms such as MD5 or SHA1.

Table 4 displays the most frequently used password algorithms from breaches where Finserv employee credentials have been exposed. Most passwords exposed are plaintext or are using a weak algorithm such as MD5 or SHA1. These constitute more than 68% of passwords exposed, as these password algorithms are more easily "crackable" for attackers. Another point of interest is the rate of exposures with "No Password", amounting to about 26% of the total. This may be due to some breaches and leakages that expose PII but do not expose any password, as is common in breaches from sites and companies in the Data Brokers sector.

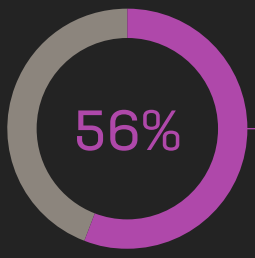
TABLE 4. MOST FREQUENTLY USED PASSWORD ALGORITHMS



Financial Services Sector Exposures: Fortune Global 500

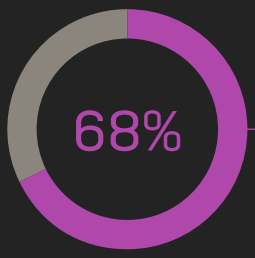
20
COMPANIES

EXPOSED IN
+6,400
BREACHES OR LEAKAGES
SINCE 2018

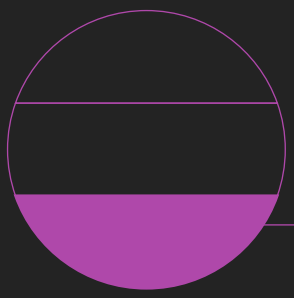


percentage of total breaches or leakages occurring since 2020

+3,360,000
RECORDS EXPOSED
SINCE 2018



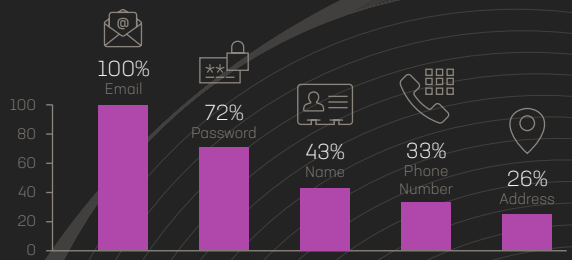
percentage of total records exposed since 2020



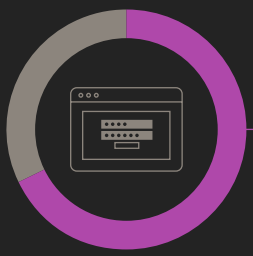
66%
BREACHES
WITH PII

More than one-third of those breaches and leakages occurred in 2021.

What PII is most commonly exposed?



Weak Password Usage



68%

of breaches are in plaintext, or use weak algorithms such as MD5 or SHA1.

Where are these breaches taking place?

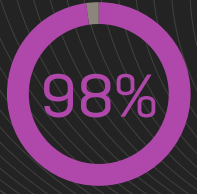
Over 30% of breaches and leakages of Finserv sector corporate credentials are from companies or sites in the U.S.

Out of a sample of 79 executives from Fortune 500 Finserv companies.

71%

had their corporate credentials exposed in a breach or leakage since 2018.

Of those exposed



98% have been exposed in breaches or leakages with PII.

2/5 have had their password exposed.

Conclusion and Recommendations

Due to hybrid, remote work models being the "new normal" into 2022 and beyond, there is little debate that threat actors will continue to target an organization's brands, employees, and executives in the Finserv sector. However, there are solutions and strategies that companies can immediately adopt to protect their executives and employees from exposures that lead to data breaches, account takeover, impersonation, ransomware and other cyberattacks.

What can organizations, executives and their employees do to reduce their collective digital risk?

1. Avoid the use of corporate email and any other related corporate credentials outside of the corporate environment. This will reduce the likelihood of corporate credentials being exposed in future data breaches.
2. Limit the use of personal data (including data related to the private or family spheres) in both the corporate environment as well as on social networks.
3. Use a secure and strong password that is consistent with the established security policies of your organization. Corporate passwords should never be used as the same password for personal accounts.
4. Continuously monitor the external threat landscape for exposed credentials and other digital threats to safeguard your employees, your brand, critical systems and assets against threat actors' attempts to exploit sensitive personal data and corporate credentials to gain access to corporate networks.

TO SAFEGUARD AGAINST THESE THREATS:

3 of the top 5 U.S. banks trust Constella Intelligence.

6 out of the top 10 global banks trust Constella Intelligence.

The trends identified by Constella Intelligence through this comprehensive analysis of breached and leaked data circulating in underground forums and the deep and dark web offer unmatched insight into the landscape of digital risks in the Finserv sector. As companies expand their digital reach, virtually all operations and communications are becoming deeply embedded within and dependent upon this shared digital ecosystem. In this environment, effectively all companies, individuals, and institutions are experiencing a dramatic expansion in their digital infrastructures, constituting an expanding attack surface and overall digital risk.

To combat these threats, it is incumbent upon companies to practice good cyber hygiene and invest in cybersecurity solutions to defeat digital risks. Constella Intelligence offers industry best products to rapidly identify threats targeting individuals to mitigate risks before any damage can occur. Constella Intelligence's Dome Executive and Employee Protection solutions allow organizations to accelerate response to digital risks, such as exposed credentials or PII in data brokers before they can be used to bypass security controls and access critical systems. Constella's platform can initiate takedown once a breach occurs, automatically blocking compromised credentials, require a password reset or additional authentication before bad actors can gain unauthorized access to critical systems.

Exposed corporate credentials of employees and executives present a greater risk than ever.

About Constella Intelligence

Constella Intelligence is a global leader in Digital Risk Protection that works in partnership with some of the world's largest organizations to safeguard what matters most and defeat digital risk. Our solutions are a unique combination of proprietary data, technology, and human expertise to anticipate, identify, and remediate targeted threats to your people, your brand, and your assets at scale—powered by the most extensive breach and social data collection from the surface, deep and dark web on the planet, with over 100B attributes and 45 billion curated identity records spanning 125 countries and 53 languages.

Our recent work has been featured in major mainstream media like the Wall Street Journal, World Economic Forum, and Forbes, in addition to other notable media.

To learn more about how you can proactively anticipate, identify, and remediate targeted threats to your people, your assets, and your brand try our Exposure Risk Tool to see if you or your company has been exposed - FREE

Why Constella

OUR TEAM

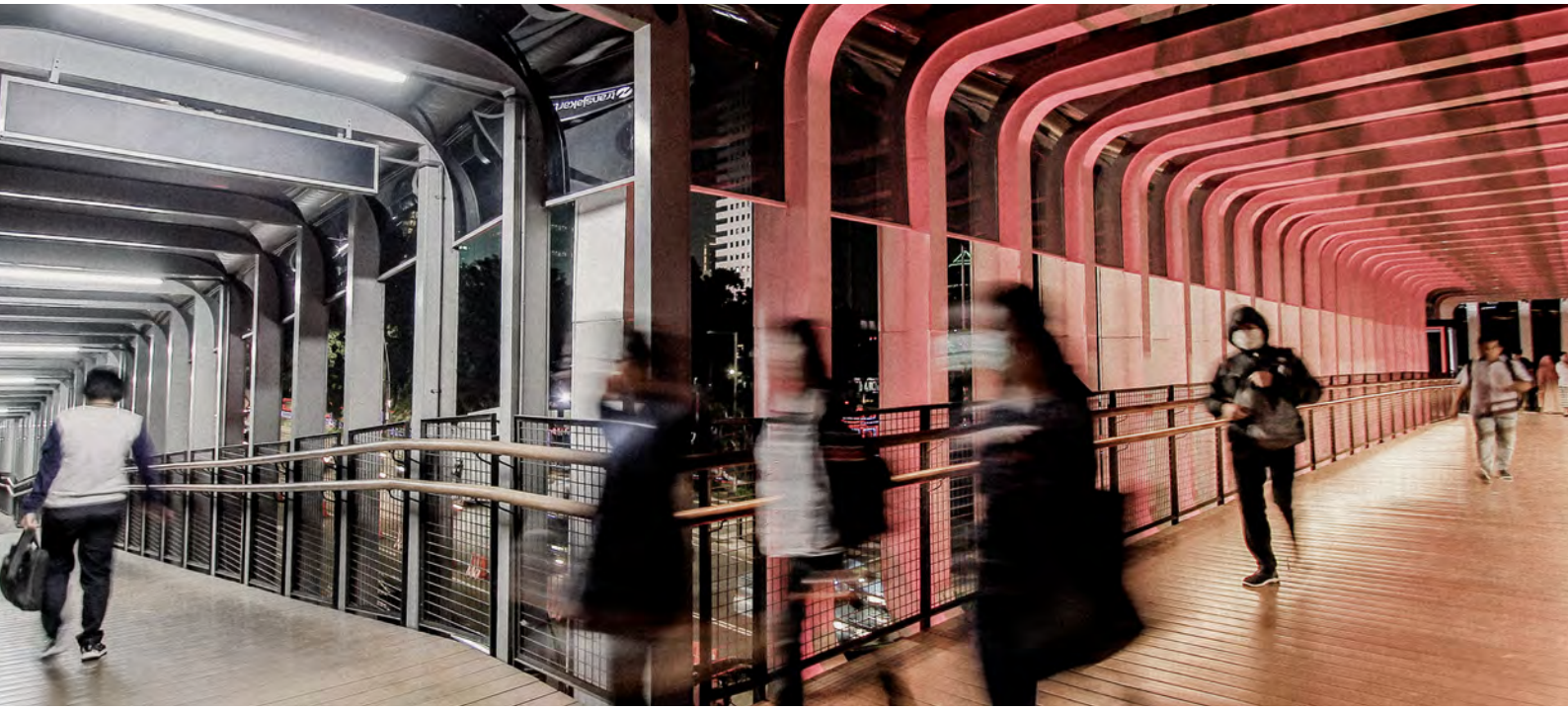
We're a diverse multinational team committed to becoming the most trusted global partner for defeating digital risk. Constella integrates interdisciplinary intelligence community analysts, infosec pioneers, military veterans, and tech entrepreneurs with advanced analysis of surface, deep, and dark web to protect what matters most.

OUR INSIGHTS

Our diverse team of expert multidisciplinary cyber intelligence analysts delivers real-time, actionable insights to identify threats and reduce risks emerging from social media, the surface, deep, and dark web.

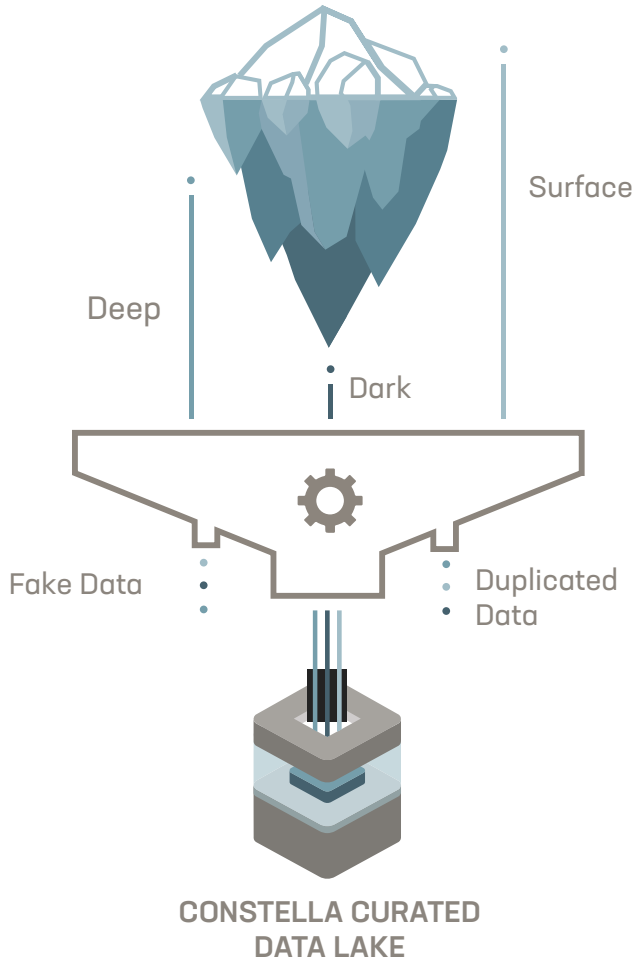
OUR DIFFERENCE

Our unique technology enables real time visibility across the entire attack surface and proactive protection against digital threats through continuous monitoring of social media, domain, surface, deep and dark web protection organizations, their employees, brand and critical assets.



Annex: Data Verification & Methodology

CONSTELLA DATA VALIDATION AND CURATION



While the number of accumulated raw identity records provides insight into the exposure of activity of identity-based data, it is not the best indicator of overall risk.

This is because not all of the data gathered is authentic or unique. After collecting the raw data, Constella Intelligence analyzes the details using machine learning algorithms, quickly identifying real (not fake) data, flags sensitive information, and removes duplicate records.

Next, breaches undergo a verification process where our analysts and experts use numerous research and investigative methods to ensure that the domain and other breach information are real and valid. The breach is then attributed and normalized.

After a breach is verified, the Constella Intelligence platform calculates a risk score based on several variables, including types of attributes, date, and password strength.