2020 in review

Data Breach Report

Released 01.28.2021

ITRC | IDENTITY THEFT RESOURCE CENTER

idtheftcenter.org • 1-888-400-5530

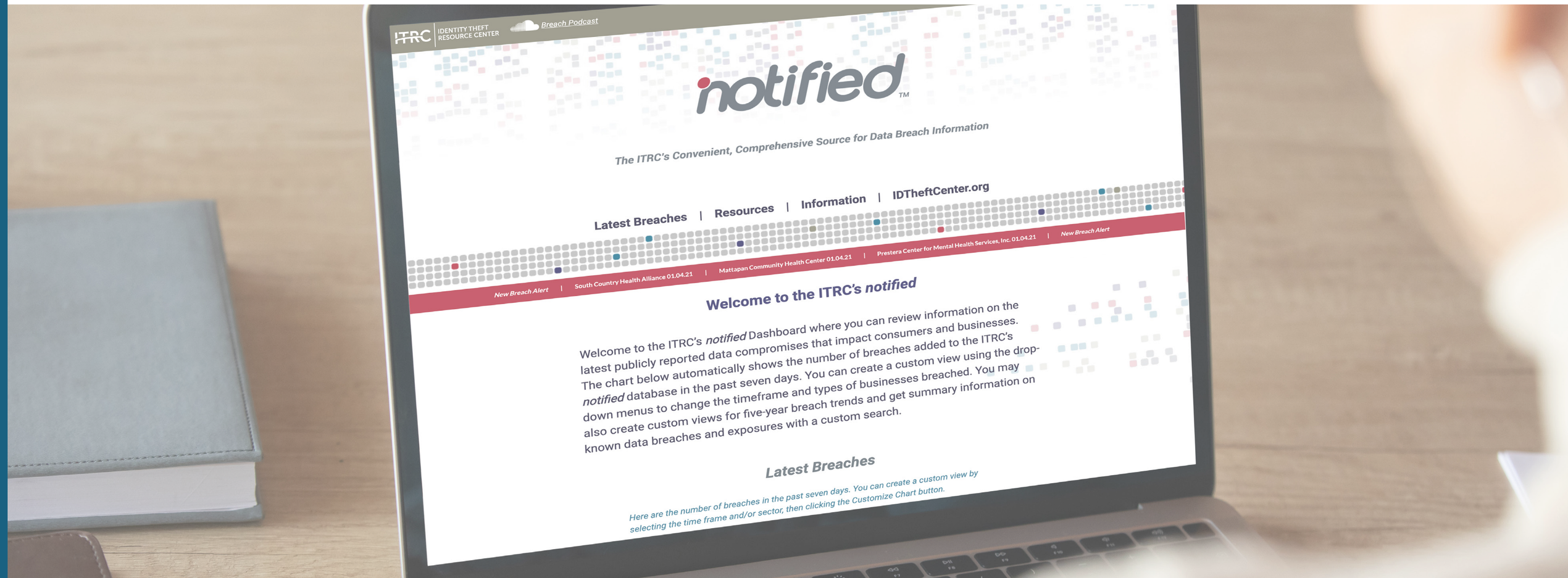
Are consumers at less risk?

Table of **Contents**

ITRC
IDENTITY THEFT
RESOURCE CENTER

Introduction

Since 2005 the Identity Theft Resource Center has tracked publicly reported data breaches in the United States. What began as a collection of basic information has grown into a database of more than **12,250** data compromises that includes up to 90 data points per event.



This report highlights a number of trends that indicate the dynamic nature of identity crimes and compromises. While one trend may be on the decline, another is on the rise. That is the nature of the never-ending contest between attackers who seek information and defenders who protect it.

Significant trends include:

- A drop in the number of data breaches coupled with a drop in the number of individuals impacted; and,

- A shift away from mass attacks seeking consumer information and toward attacks that target businesses using stolen logins and passwords

*One **troubling** trend...*

is the decreasing amount of funding available to support programs that help victims of identity crimes. The U.S. government has been the primary source of funding for victim assistance offered by the ITRC and other non-profit organizations as well as state and local government agencies. Those funds are steadily being reduced. At a time of unprecedented identity fraud related to unemployment and pandemic benefits, no federal funds were specifically awarded for FY 2020-21 to provide assistance to identity crime victims.

Executive Summary

ITRC
IDENTITY THEFT
RESOURCE CENTER

It's a cliché to point out that 2020 was an unusual year, but not always in the ways we expected. We know now that the global pandemic resulted in fundamental changes in commerce and the workplace.

Increased online shopping and remote work as a result of the response to COVID–19 dramatically increased the threat landscape that could lead to a data breach. Yet, as we'll explore in this report, the number of data breaches did not increase, and the number of individuals impacted did not grow. Just the opposite.

1108 total data breaches, down 19% compared to 2019

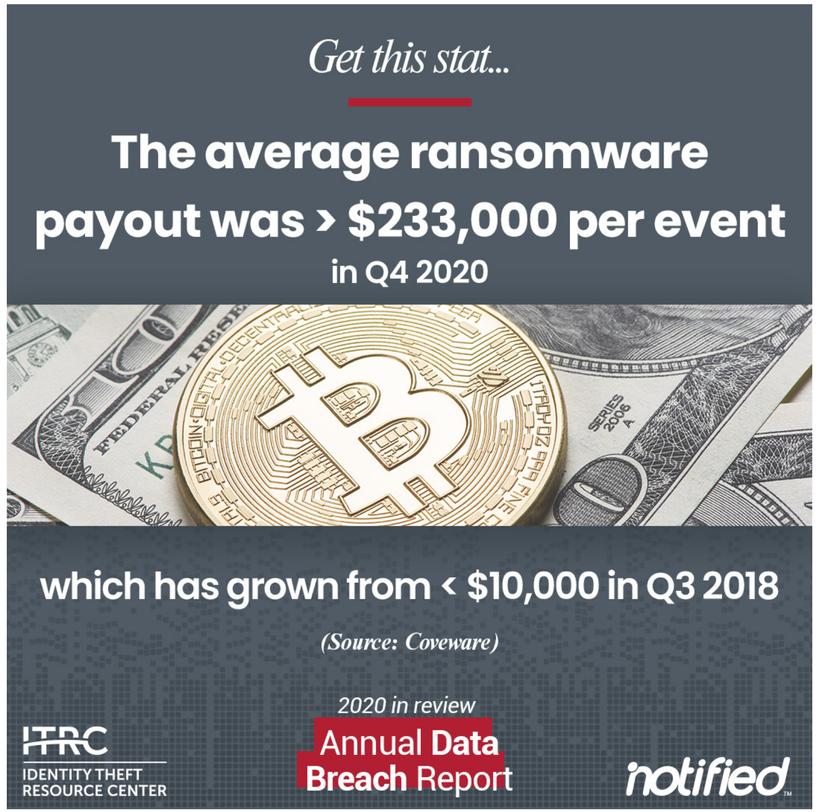
ITRC
IDENTITY THEFT
RESOURCE CENTER

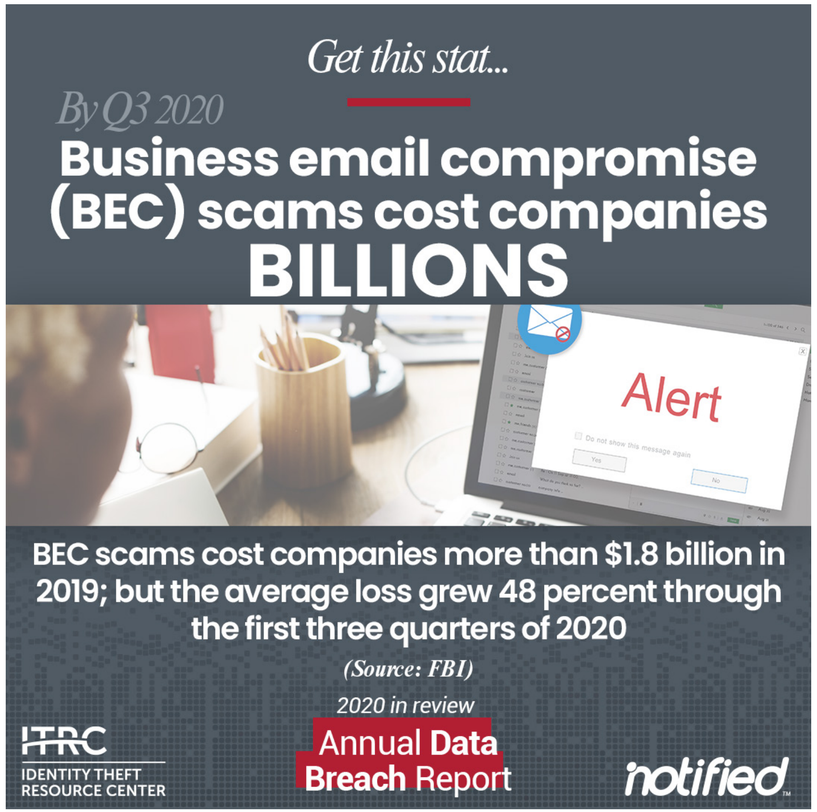
300,562,519 individuals impacted by publicly reported data breaches, down 66 % over 2019

Analysis of 2020 data breaches reveals the continuation of a trend from 2019: cybercriminals are less interested in stealing mass amounts of consumers' personal information. Instead, threat actors are more interested in taking advantage of bad consumer behaviors to attack businesses using stolen credentials such as logins and passwords.

Ransomware and phishing attacks directed at organizations are now the preferred method of data theft by cyberthieves. These attacks generally require only a stolen

credential or for an employee to click on a link in an unsolicited email, text, or social media account. Ransomware and phishing require less effort, are largely automated, and generate payouts that are much higher than taking over the accounts of individuals. One ransomware attack can generate as much revenue in minutes as hundreds of individual identity theft attempts over months or years.





"Now is not the time for consumers to think their risk has evaporated. There are still hundreds of millions of records exposed each year and consumers need to understand this is a continuing risk that can have real impacts on their lives."

– Eva Velasquez (ITRC President & CEO)

In late December 2020, threat actors believed to be affiliated with the Russian intelligence service infiltrated up to 18,000 government agencies and private sector companies through the software services of a single company - SolarWinds. At the time of this report's publication in January 2021, there was no indication consumer information, including personally identifiable information, or PII, had been stolen or compromised. In keeping with trends identified in this report, the information at risk is believed to corporate and government intellectual property. If it is later determined consumer information was compromised, the ITRC will add this breach to the data breach repository.

Our analysis does not suggest that consumers can relax as cybercriminals look elsewhere for quick, easy wins. Identity thieves still steal and misuse consumers' personal information even as the information they want and how they obtain it changes. That's why it's important for both individuals and organizations to follow good cyber-hygiene practices.

In the pages that follow, we will highlight:

- The number of data compromises
- The root causes of the data compromises, including case studies of the leading causes
- The types of data that were compromised

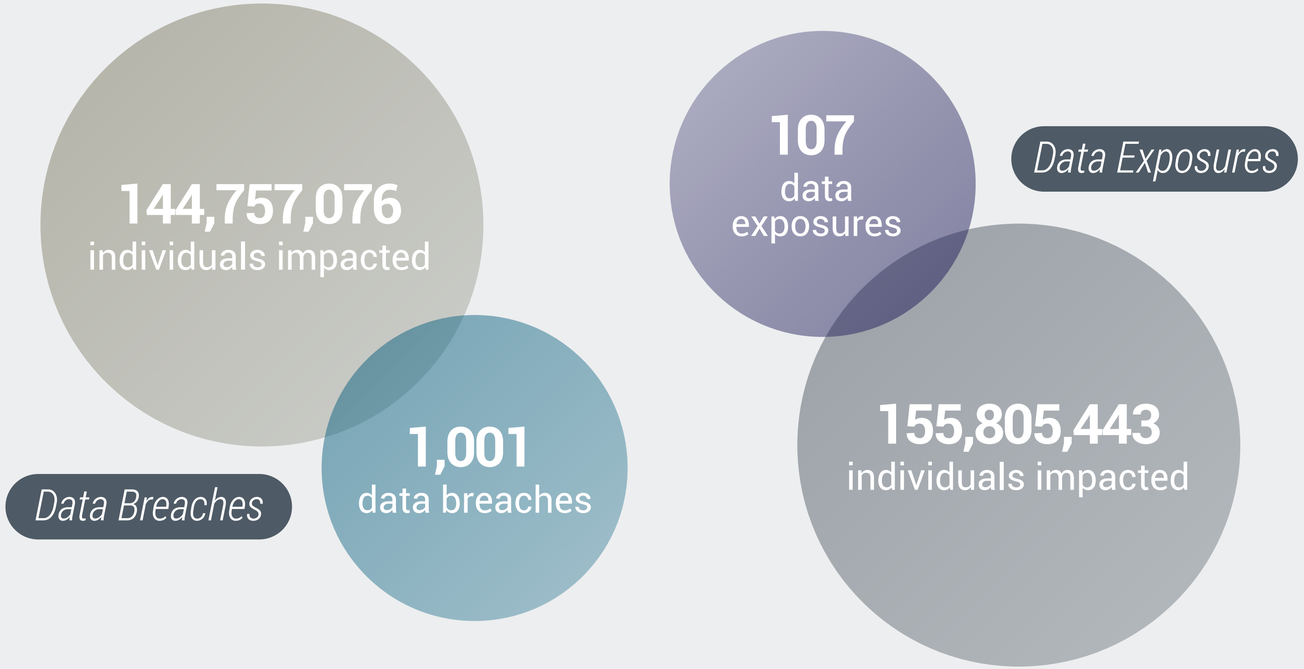
Number of **Compromises**

ITRC
IDENTITY THEFT RESOURCE CENTER

*Year-Over-Year Totals**

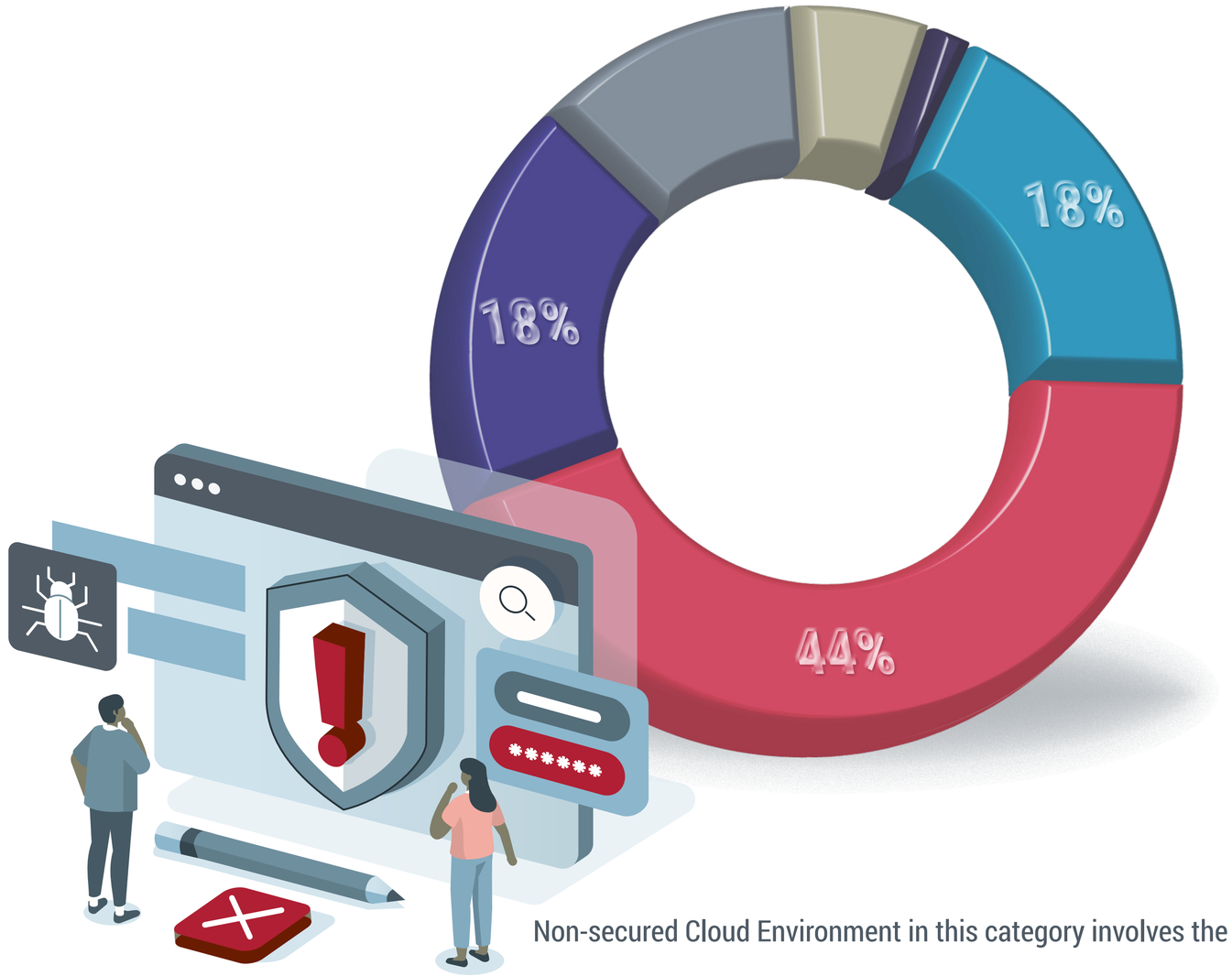
* Includes third-party/supply chain compromises as single incidents, does not include individual entities affected by a third-party compromise

	2015	2016	2017	2018	2019	2020
# of Breaches & Exposures	785	1,104	1,631	1,280	1,362	1,108
# of Individuals Impacted	318,276,407	2,541,581,891	2,081,515,330	2,231,245,353	887,286,658	300,562,519



Root Causes of **Compromises**

IDENTITY THEFT RESOURCE CENTER



Cyberattacks

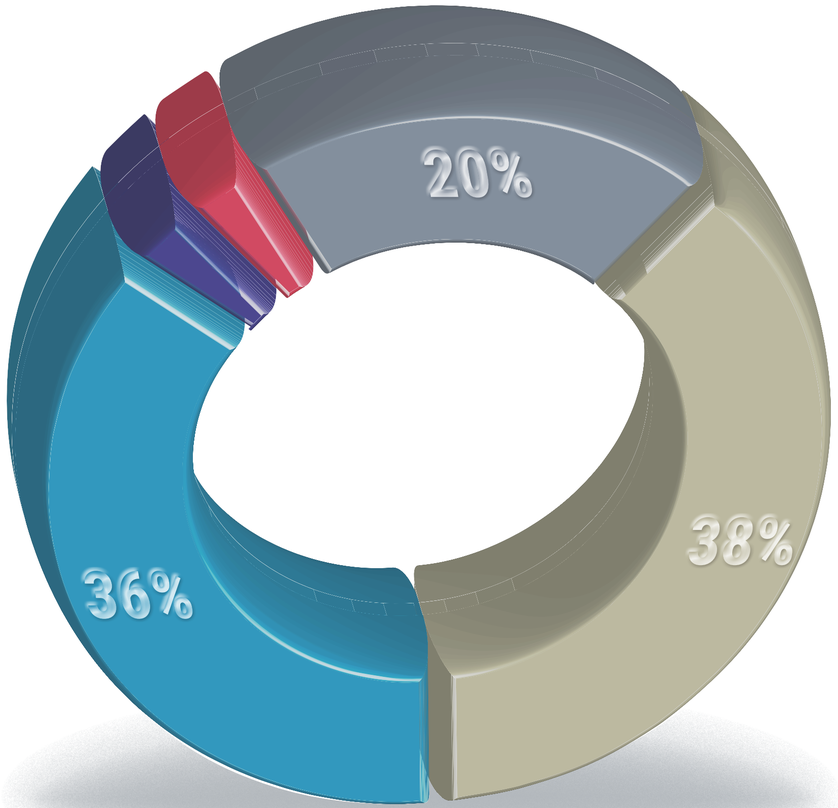
878 events

169,575,338 individuals impacted

Cause	Qty	%
Phishing/Smishing/BEC	**382**	44%
Ransomware	**158**	18%
Malware	**104**	12%
Non-secured Cloud Environment	**50**	6%
Credential Stuffing	**17**	2%
Unpatched software flaw (CVE)	**3**	0%
Zero Day Attack	**1**	0%
Other – not specified	**160**	18%

Non-secured Cloud Environment in this category involves the theft of data from a cloud data repository.

Root Causes of Compromises



Human & System Errors

152 events

130,043,536 individuals impacted

Cause	Qty	%
Failure to configure cloud security	**57**	38%
Correspondence (email/letter)	**55**	36%
Lost device or document	**5**	3%
Misconfigured firewall	**4**	3%
Other – not specified	**31**	20%

Failure to configure cloud security in this category means data was open to the internet, but there is no indication data was removed or viewed.

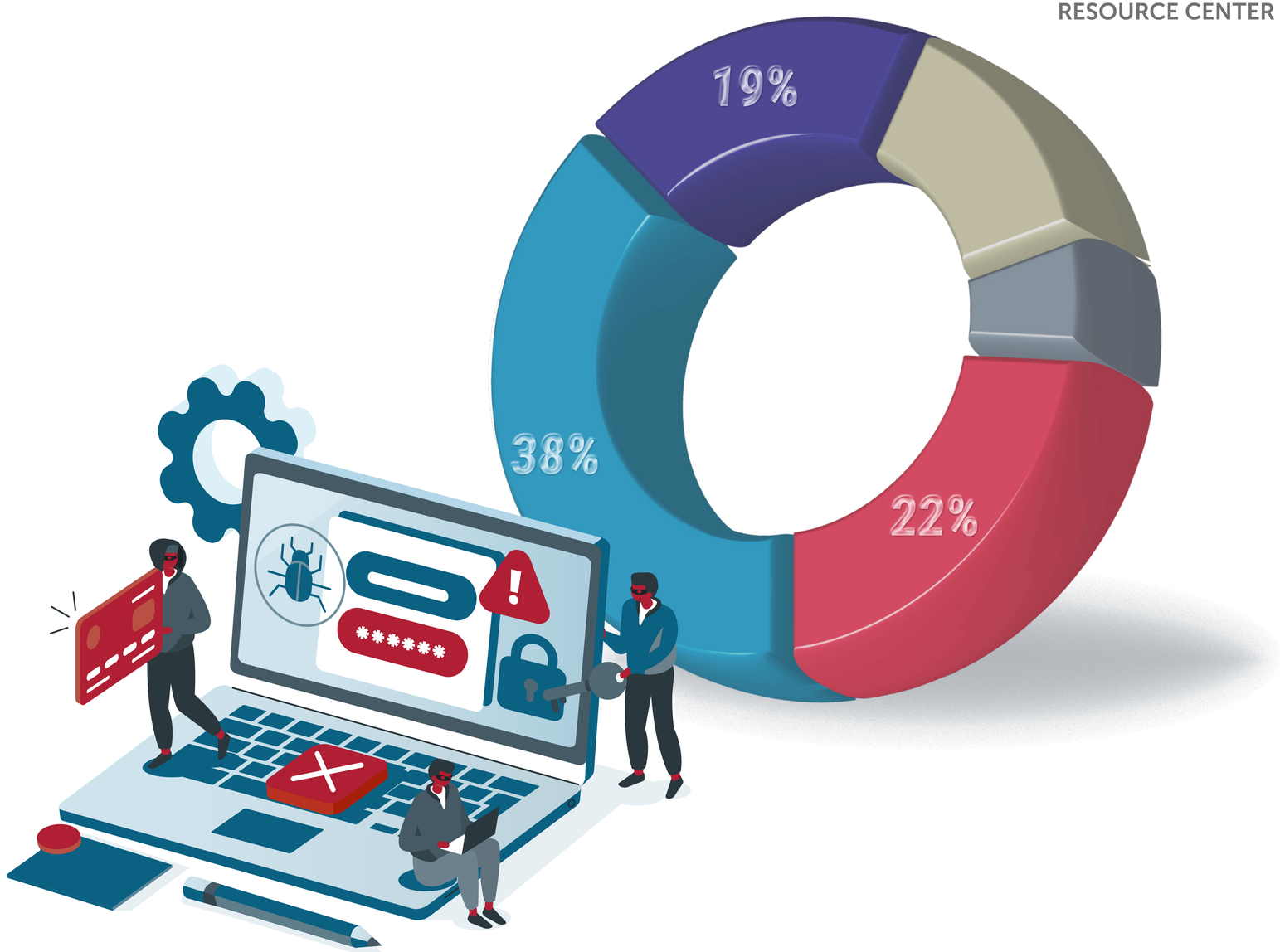
ITRC
IDENTITY THEFT
RESOURCE CENTER

Physical Attacks

78 events

943,645 individuals impacted

Cause	Qty	%
Device Theft	***30***	*38%*
Document Theft	***15***	*19%*
Improper Disposal	***11***	*14%*
Skimming Device	***5***	*6%*
Other – not specified	***17***	*22%*



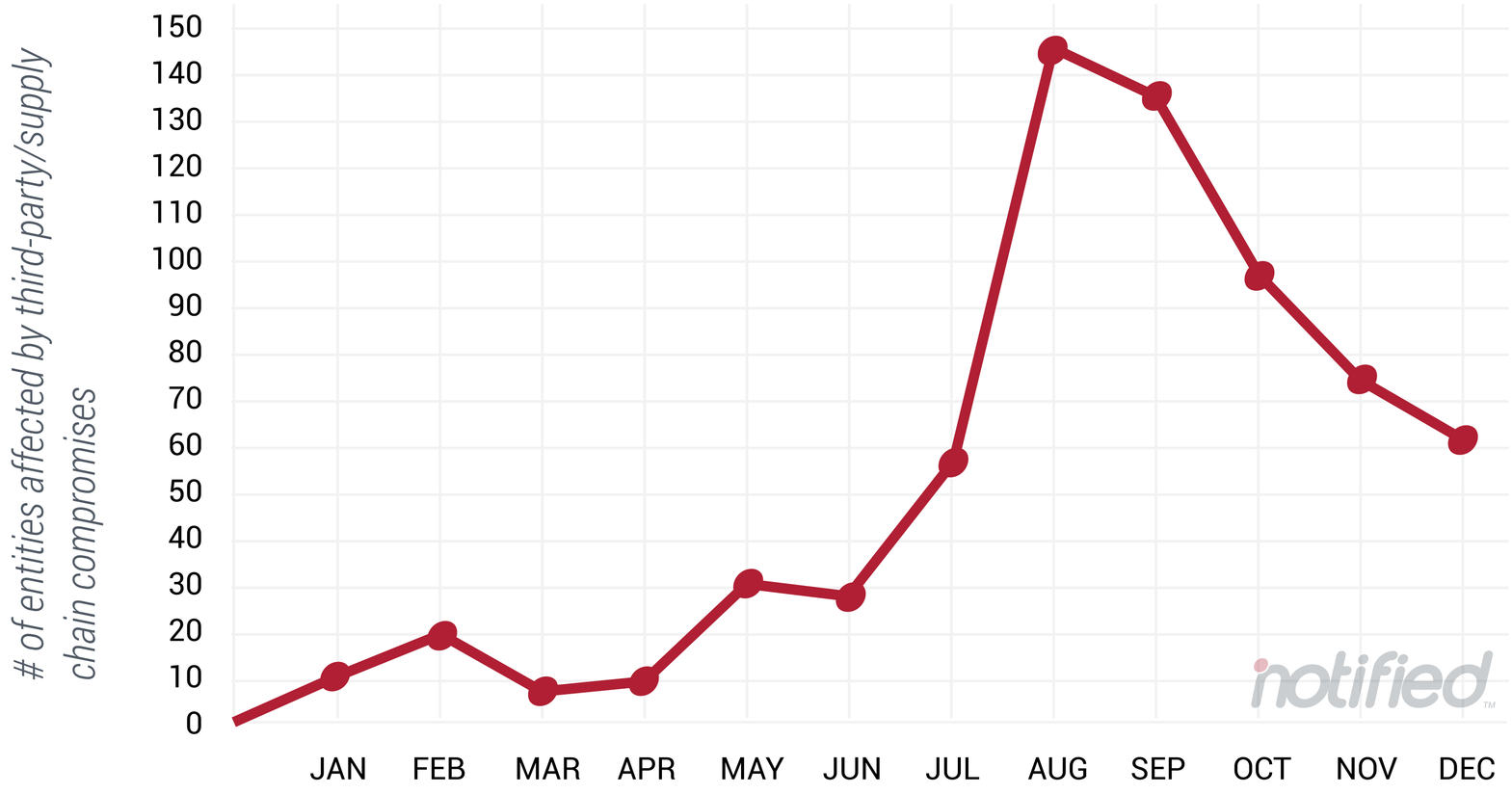
Supply Chain Attacks

694 entities affected

42,323,106 individuals impacted

Supply chain attacks are increasingly popular with attackers since they can access the information of larger organizations or multiple organizations through a single, third-party vendor. Often, the organization is smaller with fewer security measures than the companies they serve.

- 668 entities affected w/ 27,345,181 individuals impacted by third-party/supply chain cyberattacks
- 16 entities affected w/ 14,314,836 individuals impacted by third-party/supply chain system & human errors
- 10 entities affected w/ 663,089 individuals impacted by third-party/supply chain physical attacks




ITRC
IDENTITY THEFT™
RESOURCE CENTER
21 Years of Service
"The trend away from mass data breaches and toward more precise and sophisticated cyberattacks doesn't mean businesses can relax. Just the opposite. They need to learn whole new ways of protecting their data."
– James E. Lee (ITRC COO)

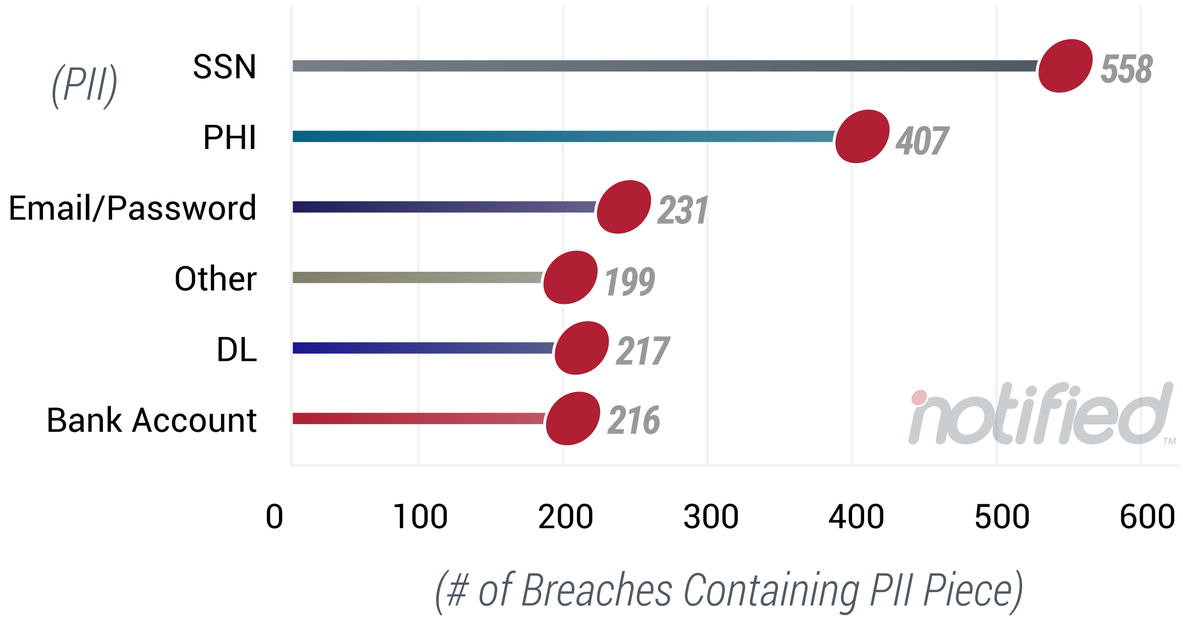
Types of **Data Compromised**

IDENTITY THEFT RESOURCE CENTER

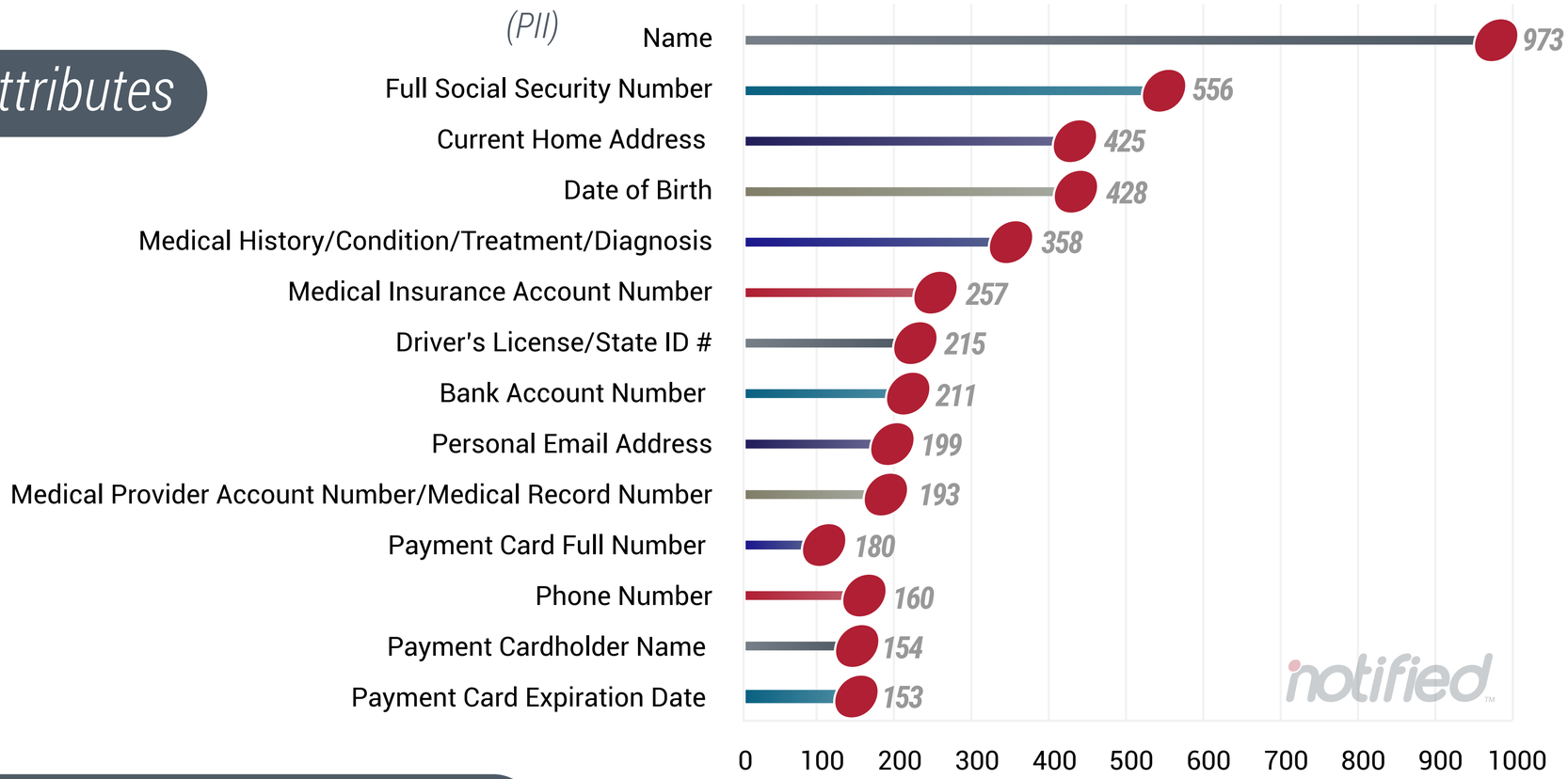
Top Breached Data Types

- *Name*
- *SSN*
- *DOB*
- *Home Address*
- *Medical History/Treatment/Diagnosis Info*
- *Medical Insurance Number*
- *State ID/Driver's License*
- *Email Address Personal*
- *Chk/Savings Account # (Bank Account Number)*

Data Exposed/Breached



Data Attributes



Other Notable Attributes < 150

Payment Card Security Code	143	Employer Contact Information	11	Loan Account Details or Credentials	4	Voter Registration Info/Preferences/Etc.	1
Undisclosed Records	109	IP Address/Device ID	10	Location	3	Merchant Login	1
Passport Number/Visitor Status/Green Card	77	Insurance Account Details or Credentials	9	Medical Insurance Account Credentials	3	Security Clearance/Access	0
Bank Account Routing Number	67	Payment Card Partial Number	8	Bank Account Login Credentials	3	Investment Account Details or Credentials	0
Other Account Credentials	65	Prior Home Address	8	W2 Other Info	3	Utility Account Credentials	0
Income/Wages/Earnings/Compensation	41	Student ID Number/Student Login/Student Details	8	Education	3	Utility Account Number	0
Employer Name	32	Financial Account PIN	6	Employer Site/System Access Credentials	2	Phone Account Credentials	0
Tax ID #	27	Medical Provider Login Credentials	6	Partial Social Security Number	2	Work Email Account Credentials	0
Work Email Address	21	Biometric/Authentication Data	5	Affiliations	1	Web History/Preferences	0
Employee ID #/Credentials/Position/Etc.	18	Friends/Family	4	Hometown	1	Credit Dispute Info	0
Other Biographical	12	Social Media Login Credentials	4	Personal Email Account Credentials	1	Non-Debit Payment Account Credentials	0

Case Studies

A. Ransomware
– *Blackbaud*

B. Stolen credentials
– *Government Benefits Fraud*
– *Unemployment Insurance*

C. Unsecured Databases
– *Vertafore*

Ransomware

ITRC IDENTITY THEFT RESOURCE CENTER

Ransomware attacks are where mass amounts of consumer or company data is held hostage under threat of public release. Sometimes the information is personal information about consumers and sometimes it is company intellectual property. In most cases, cyberthieves remove information before telling the company they have stolen valuable data that will be released to the public unless a ransom is paid.

How to protect yourself:

There is little a consumer can do to prevent a ransomware attack, but they are rarely the target. Businesses should follow best practices, including:

Frequent system back-ups

Patching software flaws as soon as notified

Not paying ransom demands

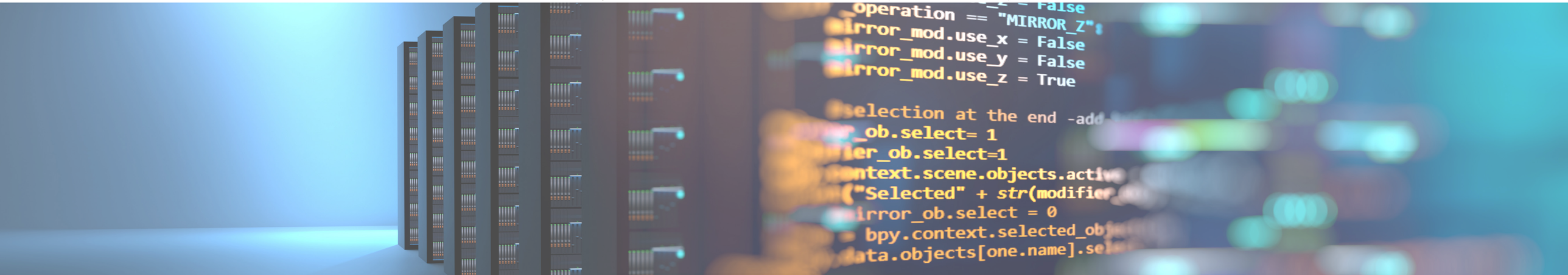
Blackbaud

What happened:

Blackbaud is a technology services company used by non-profit, health, and education organizations. A professional ransomware group stole information belonging to more than 480 Blackbaud customers before informing the company the information was being held hostage. The stolen information included personal information relating to more than 12.5 million people that was later reported to have been destroyed by the cybercriminals after Blackbaud paid a ransom.

Why it's important:

This is a good example of cybercriminals relying on an attack against a single business as opposed to a series of attacks against a large number of consumers to large sums of money.



Stolen Credentials

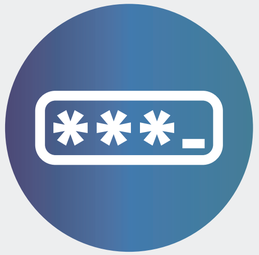
ITRC IDENTITY THEFT RESOURCE CENTER

Cyberthieves often just need login and passwords from consumers to launch attacks since people tend to re-use passwords at work and home on more than one account. More than 15 billion credentials are available for sale at any given time in underground identity markets. Consumers also willingly share them as part of phishing attacks and spoofed websites, too. Cybercriminals use automated tools that can attempt to access 500 accounts per second using stolen logins and passwords.

How to protect yourself:

At work and at home, follow best practices:

Do not reuse passwords – one unique password per account



Upgrade to a passphrase that is at least 12 characters long

Use multi-factor authentication (MFA) when possible

Consider creating online accounts so cybercriminals can't create one in your name

Use a password manager if needed

Unemployment Insurance Benefits Fraud

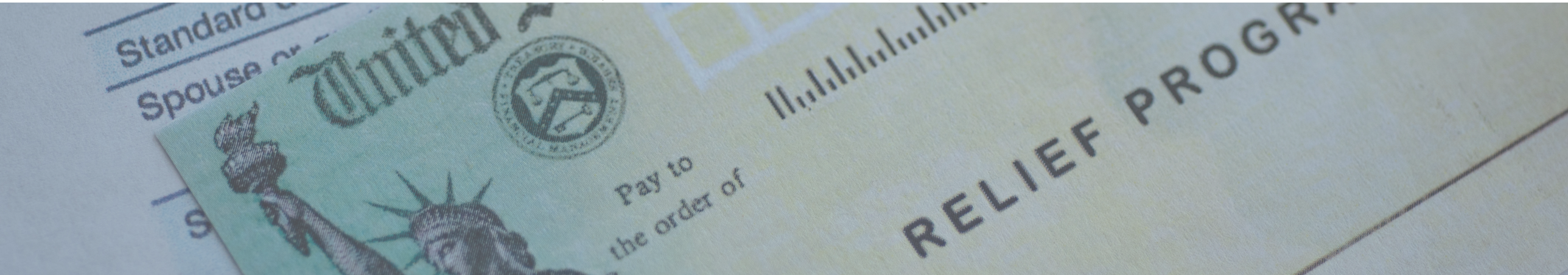
ITRC IDENTITY THEFT RESOURCE CENTER

What happened:

In 2020 organized cybercriminals used stolen credentials and other identity information to apply for unemployment benefits through state websites. Washington and Maryland each reported more than $500 million in fraudulent benefit claims. The State of California reported more than $11 billion. The U.S. Depart of Labor informed Congress that identity thieves collected an estimated $26 billion in unemployment benefit payments.

Why it's important:

This type attack proves it is easier – and more profitable - to commit a cybercrime using stolen, legitimate credentials rather than try to hack into a company's computer network.



Unsecured Databases

The best security solutions, processes, and policies can't protect you if do not configure the tools. As more organizations move their applications and databases to cloud environments, it's a common misconception that the cloud service provider is also responsible for cybersecurity. That's not true and the result is an increasing number of data compromises caused by someone failing to secure an online database.

How to protect yourself:

*If you are a consumer, use the ITRC's **notified** service to see if an organization where you have a relationship - or are considering one – has failed to secure their online databases. Businesses should follow best practices, including:*

Properly configure cybersecurity tools for cloud environments

Apply the same level of effort to protecting cloud environments as on-premise system and data assets

Vertafore

What happened:

Vertafore is a technology company that helps insurance companies price automobile insurance. Vertafore employees placed the license and related information of 28 million Texas drivers into a cloud database that was left unsecured for months. Investigators say the information was viewed by unauthorized third-parties, but there was no evidence the information was misused so far.

Why it's important:

Unsecured databases are tied for first place as the root cause of data compromises according to IBM, a statistic that is reinforced by the ITRC's analysis of 2020 data compromises. While the risk of identity crimes is low with most events where a cloud database is left unsecured, it is not zero.

Two New Podcasts

Start listening to IDTheftCenter today!

https://idtheftcenter.podsite.io/

ITRC IDENTITY THEFT RESOURCE CENTER

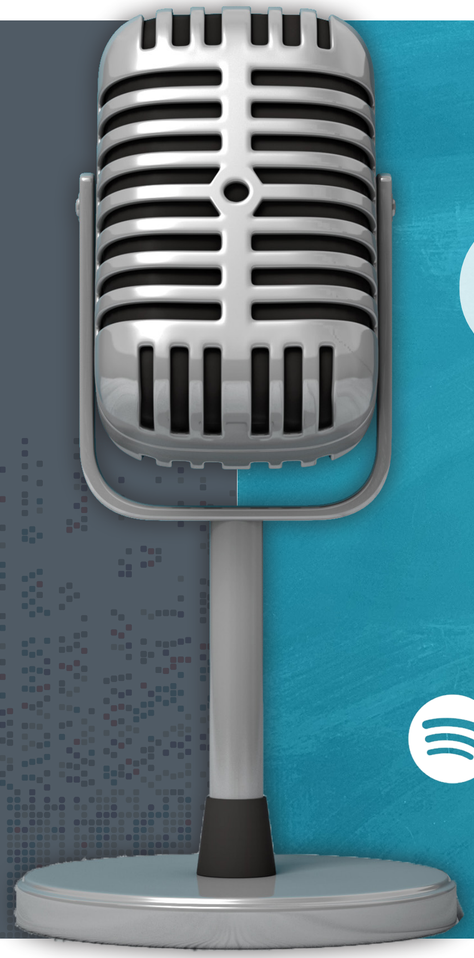
Subscribe to our feeds for trends related to Consumer and Business data security and privacy.

notified™

WEEKLY BREACH BREAKDOWN

"Ransomware and phishing require less effort, are largely automated, and generate payouts that are much higher than taking over the accounts of individuals."

– 2020 ITRC Breach Report



The Fraudian Slip

Monthly podcast
featuring fraud experts

Play, Download, or Subscribe to All Our Feeds!

Spotify®

Listen on Apple Podcasts

SOUNDCLOUD

Data Sources & Disclaimers

In conjunction with this report, we are formally launching our new data breach tracking subscription - ***notified***. Basic information is free online to consumers. Monthly and annual commercial subscriptions are available to registered businesses, government agencies, academic institutions, and non-profit organizations that need data breach information for strategic planning, vendor due diligence, and trend analysis. You can register for our monthly updates, quarterly reports, and business subscriptions at **notified.idtheftcenter.org**.

The ITRC gathers information about publicly reported data breaches from a variety of sources including: company announcements, mainstream news media, government agencies, recognized security research firms and researchers, and non-profit organizations. The ITRC accepts these reports "as is" and makes no warranty as to their accuracy or completeness.

It is common for the number of individuals impacted to change over time. Initial reports are often based on incomplete or inaccurate information resulting in the number of impacted individuals, the root cause of the data breach, and the cost of the data breach to the breached company among other factors to require occasional updates.

Different states have different reporting requirements. This often results in time lags between the time a government official is notified of a data breach and when the breach is officially reported. There are also variations in data breaches are defined and what data is governed under a given state's laws, resulting in data being subject to a breach notice in some states, but not all.

There are a number of for-profit and non-profit organizations that publish data breach information, but each organization captures and views the information differently. There are four key differences in how the ITRC reports data breach information:

- The ITRC only publishes data related to publicly reported U.S. compromises
- The ITRC focuses on the number of individuals impacted, not the number of records exposed in keeping with our mission of a victim assistance organization
- We make a distinction between data breaches, where information is removed and/or misused, and data exposures where information is not secured but there is no evidence it has been removed or misused.
- We do not report data breaches where the information is not protected under a state's data breach notice law

A Special Note About Supply Chain Attacks

Supply Chain Attacks happen when a cybercriminal targets a vendor who has access to a larger organization's information or a business that holds the valuable information of multiple organizations. One of the trends masked in this year's data compromise data is the depth and breadth of the impact of these attacks.

For purposes of reporting data breaches, only the breached organization is reported as being compromised. However, those single events impact multiple organizations and consumers whose information is stored or accessed by the breached company. If reported as separate events, the number of Supply Chain Attacks would have been significantly higher.

You can learn more about how we define our terms and organize our data at our ***notified*** **website**.

Timely, comprehensive breach information at your finger tips

notified.idtheftcenter.org • notifiedbyITRC@idtheftcenter.org

notified™

The ITRC's Convenient, Comprehensive Source for Data Breach Information

ITRC | IDENTITY THEFT RESOURCE CENTER

idtheftcenter.org • 1-888-400-5530