# Data Breach Industry Forecast 2020

By Experian® Data Breach Resolution

# Executive Summary

It didn't take long for cybercriminals to say 'Happy New Year' to 2019 as the first data breach announcement came on January 2 by Blur, a password management company, that had an unsecured server exposing a file containing 2.4 million user names, email addresses and other information.

While 2018 hit record-setting numbers as to the number of data breaches and consumer records exposed, 2019 was on pace as of mid-year to be the worst year ever, according to a report by Risk Based Security.[1]

As a new decade nears, with approximately 10,800 data breaches occurring in the last 9 years, the question remains: How do we stop data breaches? While a data breach is probably inevitable, we must not throw in the towel. Companies should prioritize data breach prevention as well as response, and now take it to the next level. It's not acceptable any more to simply focus on security and hope for the best. There are additional steps organizations can take ahead of time such as investing in employee training to shore up the company's defenses, keeping up on the latest threats, securing agreements with outside partners such as legal and other experts to be at-the-ready if a breach occurs, and following new legislation such as the General Data Protection Regulation. All of these steps creates a better security poster and smoother and swifter response if a data breach happens, which will go a long way to repair brand reputation.

In our seventh annual edition of this Data Breach Industry Forecast, we address fresh real estate and audiences that hackers can target such as the cannabis industry and online communities, and vulnerabilities in popular technology that criminals could use for bad intent such as leveraging drones.

Experian Data Breach Resolution outlines five predictions for the data breach industry in 2020. We also look back on our predictions for 2019. Our predictions are rooted in Experian's history of helping companies navigate more than 30,000 breaches over the last 15 years.

## Based on our expertise, the top data breach trends of 2020 include the following:

» Cybercriminals will leverage text-based "smishing" identity theft techniques to target consumers participating in online communities, such as those supporting presidential candidates, with fraudulent messages disguised as fundraising initiatives.

» As cities install more free public Wi-Fi systems hackers will take to the skies via the use of readily available drones to steal consumer data from devices connected to unsecure networks on the streets below.

» Cybercriminals will use so-called "deepfake" video and audio technology to disrupt the operations of large commercial enterprises, and potentially create geo-political confusion among nation states, in addition to disruption in financial markets.

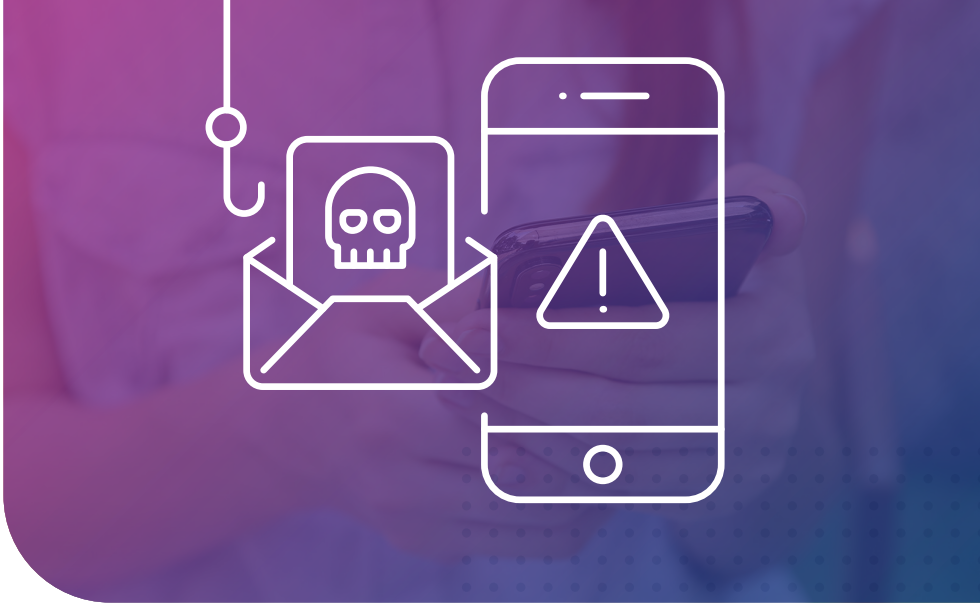
» As a form of protest, we will see many burgeoning industries, such as cannabis retailers, cryptocurrency entities, and even some environmental organizations, targeted for cyberattacks as a result of online activism or "hacktivism."

» With mobile payment options popping up everywhere from a local café to the beer vendor at a stadium, we predict that there will be a significant spike in identity theft as cyber criminals seek to exploit the convenience of point-of-sale transactions, especially at large venues like concert festivals and sporting events.

[1] 2019 MidYear QuickView Data Breach Report, Risk Based Security, August 2019

#1

# Phishing 2020



## PREDICTION

Cybercriminals will leverage text-based "smishing" identity theft techniques to target consumers participating in online communities, such as those supporting presidential candidates, with fraudulent messages disguised as fundraising initiatives.

Social media is becoming more and more fragmented as people seek out communities where they can share their experiences with like-minded followers. These communities, whether in support of a recording artist, social issue or political candidate, are creating a new form of online tribalism. As a member of the "tribe" barriers to trust – that typically safeguard us from online scams – can get lowered, especially when we think we are communicating with a fellow, like-minded member.

For example, an email or text seeking an urgent donation to a political candidate a consumer supports – using a credit card attached to a consumer's mobile phone account – may result in an immediate payment, and it may not be as real as a consumer thought.

**"Phishing" as a form of identity theft has been around since the dawn of social media, but as more and more Americans join like-minded groups on social media, a new pool of potentially unsuspecting targets is developing that can easily be manipulated by cybercriminals.**

Prior targets like banks have found ways to educate consumers on how to recognize bogus sites or email solicitations seeking account information, but more and more of today's online communities are communicating via text, and that can be more easily manipulated.

In fact, the FTC even has a new phrase for describing this wave of text-based cybercrime – "smishing" (phishing attempts that are sent through SMS text). As candidates build out online communities, a campaign page can be easily spoofed – soliciting donations via a fake email, and a "smishing" text message designed to look like it comes from a fellow campaign supporter can gain trust even faster.

### The Takeaway:

It will be important, particularly as we head into an election year, for consumers to be aware of 'smishing' (SMS phishing) attempts from hackers who may pretend to work for a political organization and ask for donations through a fake link or website. Signs of smishing scams are similar to the traditional phishing emails you may receive including misspelled words, poor grammar and requests for personal information such as your social security number, credit card or bank account information. A good rule of thumb is to refrain from responding to text messages from unknown senders.

#2

# Hacker in the Sky with Data

## PREDICTION

As cities install more free public Wi-Fi systems hackers will take to the skies via the use of readily available drones to steal consumer data from devices connected to unsecure networks on the streets below.

Over the past few years, public Wi-Fi networks have faced increasing attacks as cybercriminals used tools like Wi-Fi Pineapple technology to steal data from unsuspecting users. The Pineapple is a hand-held device that individual hackers (and cyberthieves) can purchase for about $99 on the Hak 5 website. While originally developed to be used by security professionals - the "good guys" - to help spotlight how too many unsecured Wi-Fi networks were easily subject to "spoofing attacks," it soon fell into the hands of cybercriminals.

With the device in hand, a cybercriminal can easily steal sensitive data, like passwords to an online bank account, from nearby users connected to unsecured Wi-Fi networks, such as at a conference or a coffee shop. The device, while certainly useful to security professionals testing the integrity of Wi-Fi networks, is legal for anyone to buy, and at just $99 it's been very tempting to bad actors.

However, as more and more cities install mobile hot spots in busy urban areas such as parks, stadiums and business districts, the pool of unsecured online targets has gotten far deeper. Given the size of the Pineapple device it would not be complicated for a cybercriminal to attach the device to an equally inexpensive drone device. There are currently more than 1 million drone devices legally operating in the U.S. today and the market for drone devices is predicted to get close to $100 billion by the end of 2020.[2]

**As the use of drones becomes more ubiquitous, that buzzing sound you hear overhead may not be the result of an amateur photographer seeking that perfect aerial shot or an e-commerce package getting delivered. It just might be a flying Pineapple looking to see if you have taken advantage of a free, unsecured network as you casually walk down your street with an internet-connected device in hand.**

### The Takeaway:

To keep sensitive data on your smartphone secure from drones and other aerial devices, it is important to use Wi-Fi wisely. Accessing public Wi-Fi in areas such as malls, parks and even coffee shops can open the door to hackers stealing your personal information in a matter of seconds. Implementing two-factor authentication and password protection can help minimize your risk of becoming a victim.

[2] Goldman Sachs Research

#3

# It's a Fake!

## PREDICTION

Cybercriminals will use so-called "deepfake" video and audio technology to disrupt the operations of large commercial enterprises, and potentially create geo-political confusion among nation states, in addition to disruption in financial markets.

The phrase deepfake was first coined by users on Reddit in 2017. The Artificial Intelligence–based technology was first developed in the mid-1990s as a result of academic research into computer vision, an interdisciplinary science that studies how computers can gain high-level understanding from digital images, allowing machines to perform visual tasks once left to humans. However, in recent years the technology has been used by amateurs and even cybercriminals for illicit purposes, including swapping the faces of celebrities into online pornographic videos.

The technology has also been used to cause disruption in politics. For example in a 2018 post the face of German Chancellor Angela Merkel was replaced by Donald Trump. Perhaps most famously, a 2018 video "public service announcement," ostensibly from former President Barack Obama appeared online with an altered audio track recorded by actor/director, and Obama impersonator, Jordan Peele. The video, which went viral made the case that the images and voices of world leaders could easily be manipulated and altered to cause discord and confusion. In 2019, dozens of media outlets reported on an altered video of House Speaker Nancy Pelosi that appeared to show her slurring her speech.

**Industry researchers have noted that the technology required for these audio-generated attacks has made transformative progress as a result of breakthroughs in how algorithms can be used to process data.**

As this technology comes of age and becomes readily accessible it will increasingly be used by cybercriminals and nation states to foster real disruption – both in financial markets and in politics.

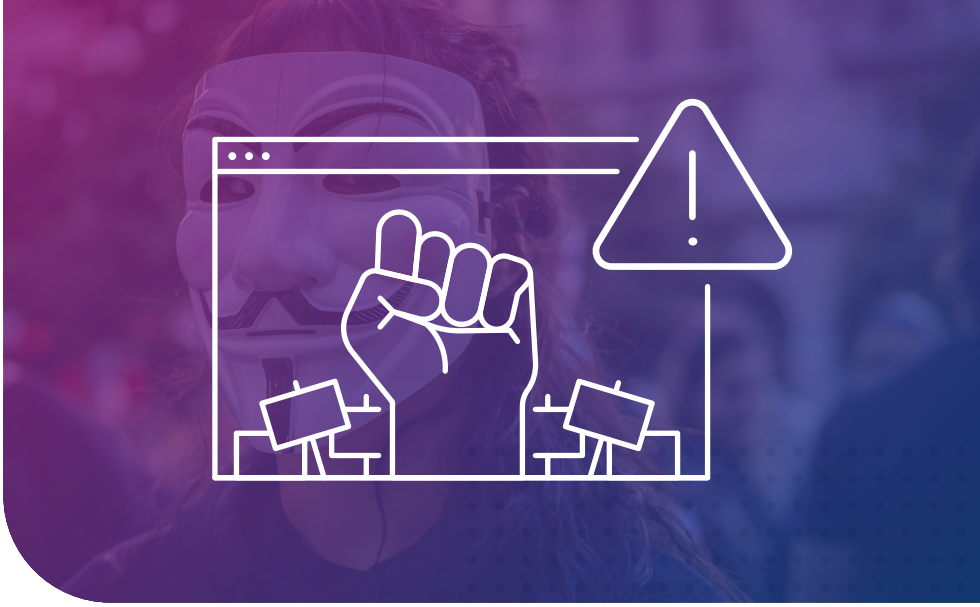
In fact, in the last year at least three cases have been reported where manipulated executive voices were used to steal money from U.S. companies. The challenge for security professionals is that the tools to defend against deepfakes are few and far between, and the challenge of quickly detecting one before any damage is done is increasingly unlikely.

### The Takeaway:

Similar to fake news, deepfake video and audio technology can be used to rapidly spread misinformation about corporations, C-suite executives and government leaders, blurring the lines between what's real and what isn't. You can detect a deepfake video by looking out for blurring in an individuals face, changes in skin tone and irregular blinking (hint: the deepfake algorithm causes people in deepfake videos to barely blink).

#4

# Going Up in Smoke



## PREDICTION

As a form of protest, we will see many burgeoning industries, such as cannabis retailers, cryptocurrency entities, and even some environmental organizations, targeted for cyberattacks as a result of online activism or "hacktivism."

Online hacktivism is not new. The earliest hacktivist attacks date back to the mid-1990s and tended to focus on the desire for political change or a position on social issues. However, due to the plethora of burgeoning and potentially controversial companies that are operating in young and rapidly growing industries, a sea of new targets exists for both activists and bad actors to target.

Many burgeoning companies, like cannabis retailers, may not fully invest in protective, cybersecurity measures as core parts of their business models due to competing priorities. While any retailer is always a target for cybercriminals, cannabis retailers present a bigger target due to the nature of their business. And medical marijuana dispensaries may be an even bigger target due to the ready access they may provide to personal medical records, many of which may prove to be very valuable on dark web forums. According to a report by Grand View Research, Inc., the legal marijuana market was estimated at 13.8 billion in 2018 and is expected to reach 66.3 billion by the end of 2025, showing the industry is budding with opportunity.[3]

**What's more, cryptocurrency exchanges are likely to become lucrative targets. Early this year one exchange experienced a breach where hackers were able to steal over 7,000 Bitcoin – worth more than $41 million at the time.**

Due to the relative youth of these burgeoning companies, hackers will be able to leverage more traditional exploits like phishing to gain access to sensitive data. What's more, the nature of their business models make these companies targets for hacktivist activity from those who simply don't agree with the company's business model.

### The Takeaway:

Cannabis retailers, cryptocurrency entities, and environmental organizations are attractive targets for cybercriminals due to their prevalence in society and increased cash flow. However, these industries are faced with many of the same cyberthreats as other businesses, such as phishing scams, cloud vulnerabilities and ransomware. That's why it's especially important for businesses that are new to the market to take protective measures such as investing in anti-malware software and implementing mandatory cybersecurity training programs for employees, to safeguard from cyberattacks.

[3] Legal Marijuana Market Size, Share & Trends Analysis Report By Type, By Product Type, By Medical Application And Segment Forecasts, 2019 – 2025, Grand View Research, May 2019

#5

# Data Here, Get Your Data Here!

## PREDICTION

With mobile payment options popping up everywhere from a local café to the beer vendor at a stadium, we predict that there will be a significant spike in identity theft as cyber criminals seek to exploit the convenience of point-of-sale transactions, especially at large venues like concert festivals and sporting events.

The mobile payments industry is expected to reach more than $4.5 trillion by 2023.[4] But with increased convenience comes threats such as e-skimming, which can happen just as easily through mobile apps as they do online. There are also real concerns about the security and privacy of some mobile payment platforms, especially at the point of sale. As small retailers, sporting venues and others install mobile point-of-sale platforms to keep up with consumer demand they may not even know that the device they've installed is not secure.

**Today, consumers expect to have the option to pay with a mobile option virtually everywhere, and where they can't use an app on their phone they expect to be able to seamlessly swipe their credit card through a vendor's handheld payment device.**

But while NFC mobile payment apps tend to carry strong security protocols, platforms that allow consumers to swipe their card through a mobile device may not be. Many of these mobile point-of-sale platforms (mPOS), due to their low cost and ease of use, often don't come with robust security features built in. With mPOS devices available to merchants for as little as $50, convenience and cost efficiencies could open the door to exploits like tampering with transaction amounts or basic identity theft.

We don't see a return to paying with cash, but consumers, merchants and venues are going to need to be increasingly vigilant and remember that the next time they hear a vendor shout "Beer here!" a cybercriminal may not be far away, and what they're hearing is "Data here! Get your data here!" If consumers don't check the mobile receipt on their phone to ensure the charge is right, it might be game over, cybercriminal wins!

### The Takeaway:

Mobile payments are here to stay, but in a rush to adopt these new payment platforms retailers need to be careful that they don't take one step forward and two steps back when it comes to security, and consumers need to be vigilant, too. The convenience of mobile payments may be an effective lure for both retailers and consumers, but both need to be careful they don't end up on the hook of a cybercriminal.

[4] Mobile Payment Market - Global Opportunity Analysis and Industry Forecast, 2016-2023, Allied Market Research, February 2018

# 2019 Forecast Scorecard Ratings

**A**

## Attackers will zero in on biometric hacking and expose vulnerabilities in touch ID sensors, facial recognition and passcodes.

### UPDATE

In 2019 we learned that Biometric security measures may not be as secure as we thought. According to an article in The Guardian, a security flaw in Biostar 2, a biometric system used by banks and commercial buildings around the world, left the fingerprints of more than 1 million people, along with facial recognition data and other personal information like user names and passwords, unprotected on a publicly accessible database. While the data was found by independent security researchers, cybercriminals could easily have accessed the data. Biometric security systems remain difficult to hack, but nothing is bulletproof, and human error will always be an issue.

**B**

## Skimming isn't new, but the next frontier is an enterprise-wide attack on a major financial institution's national network, which could result in millions in losses.

### UPDATE

O.K. This hasn't happened exactly as we predicted. Large financial institutions are successfully fighting off hundreds of attempted attacks every day. In fact, there were more than 3,000 successful attacks against financial institutions in 2019, according to the Treasury Department's Financial Crimes Enforcement Network. And there was even some good news as Russian hacker Andrei Tyurin, who had accessed more than 80 million accounts at JP Morgan Chase a few years ago, was finally arrested. However, a flaw in the security software used by Capital One allowed a hacker to gain access to the personal information of more than 100 million customers – one of the top 10 cyberbreaches of all time. Happily there were no successful attacks on a national network in 2019, but financial institutions need to stay on high alert.

B

## A major wireless carrier will be attacked with a simultaneous effect on both iPhones and Android, stealing personal information from millions of consumers and possibly disabling all wireless communications in the United States.

### UPDATE

Phew! This didn't happen. Or did it? It's true that no wireless network was disabled following an attack, but is that what cybercriminals wanted? Industry researchers say hacking activity targeted towards mobile phones increased more than 50 percent in 2019, especially as cybercriminals used malware in attempts to gain access to things like mobile banking data.[5] Attacking individual phones may prove more profitable than taking down an entire mobile network. But mobile carriers were not immune, in fact Sprint reported a breach over the summer that exposed an undisclosed number of customer login data to hackers.

A

## It's only a matter of when, not if, a top cloud vendor will suffer a breach, compromising the sensitive information of major companies.

### UPDATE

Researchers at the cybersecurity research firm ProofPoint found that cybercriminals have accessed the cloud networks of a startling 60 percent of top US companies, with over 15 million login attempts to Fortune 500 cloud networks in just the first six months of the year (400,000 were successful).[6] The massive Capital One attack was cloud based. In fact, the hacker charged in connection with the attack was accused of similar cloud breaches targeting at least 30 other companies, using a program to scan cloud customers for a specific firewall misconfiguration.

A-

## Friends or foes? The online gaming community will be an emerging hacker surface, with cybercriminals posing as gamers and gaining access to the computers and personal data of trusting players.

### UPDATE

It wasn't Game Over, but 2019 saw its fair share of cybercriminal activity in the online gaming world. Emuparadise, a retro gaming website, revealed a breach that exposed account information for more than one million users. And an irritating cyberwar on gamers was declared via a DDoS attack on servers hosted by Blizzard Entertainment, an American video game developer, during the weekend release of its "classic" edition of the hugely popular World of Warcraft, disrupting play for American and European gamers.  As this report was going to press, a data breach of publisher Zynga was announced  in October, affecting more than 200 million players.

[5] Cyber Attack Trends: 2019 Mid-Year Report, Check Point, July 2019
[6] Cloud Attacks Prove Effective Across Industries in the First Half of 2019, Proofpoint, September 2019

## About Experian Data Breach Resolution

Experian Data Breach Resolution, powered by the nation's largest credit bureau, is a leader in helping businesses prepare for a data breach and mitigate consumer risk following breach incidents. With more than a decade of experience, Experian Data Breach Resolution has successfully serviced some of the largest and highest-profile data breaches in history. The group offers swift and effective incident management, notification, call center support, and fraud resolution services while serving millions of affected consumers with proven credit and identity theft protection products. Experian Data Breach Resolution is active with the International Association of Privacy Professionals, NetDiligence, Advisen, the Ponemon Institute RIM Council, and is a founding member of the Medical Identity Fraud Alliance.

**For more information, visit Experian.com/DataBreach and follow us on Twitter @Experian_DBR.**