IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

IT Security

Expert Witness: Delivering Evidence from the Dark Web when Data Breaches Go to Court

Austin Berglas

Austin Berglas
Global Head of
Professional Services
BlueVoyant

Biography

*Austin Berglas is Global Head of Professional Services at cybersecurity specialists BlueVoyant (*https://www.bluevoyant.com/*). Austin comes to BlueVoyant after building and leading the Cyber Defence practice at K2 Intelligence. Prior to K2 Intelligence, he served 22 years in the U.S. Government.*

Austin was the Assistant Special Agent in charge of the FBI's New York Office Cyber Branch. There, he oversaw all national security and criminal cyber investigations in the agency's largest cyber branch, and was awarded the FBI Director's Award for Excellence in a Cyber Investigation. Prior to the FBI, Austin achieved the rank of captain in the U.S. Army.

Keywords Cybersecurity, Data breach, Risk, Expert witness, Legal, Personally Identifiable Information (PII)
Paper type Opinion

Abstract

With personal data being easily purchased from the dark web. Many criminals are undertaking this data to commit identity theft but BlueVoyant professions can evaluate and explain to courts how personal data is sourced by cybercriminals and used to commit fraud. In this article the author discusses how the impact of stolen data can become a legal issue in terms of class action lawsuits.

Introduction

The well-publicized implementation of privacy legislation, including the California Consumer Privacy Act (CCPA) and General Data Protection Regulation (GDPR), has raised public awareness considerably regarding the value of personal data and the implications of its loss or theft. The fear that a malicious actor might use stolen Personally Identifiable Information (PII) or other personal data to commit fraud via identity theft is a real and understandable concern for individuals. This fear is compounded by the frequent data breaches that hit the headlines, where people hear or read about millions of records being exposed or stolen. Often, one outcome of these mega breaches is a class action lawsuit, where individuals whose data has been breached launch a suit against the organization that has been accused of not securing their data.

As experts in cybersecurity and the dark web, where breached data is often destined to end up for sale, BlueVoyant professionals may be called in as expert


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

witnesses to help analyze the risk increase a breach has, or has not caused, and explain to the court how personal data is sourced by cybercriminals and used to commit fraud. So, what are some of the factors we consider when we assist in these cases and how can individuals minimize their risk of fraud, even if their data is involved in a breach?

The first thing to note is that no one wants to end up on either side of a class action lawsuit over a data breach. Plaintiffs are worried about whether they need the protection of anti-fraud measures, and defendants have suffered loss of customer trust, reputation, and potential financial damage. We focus on helping courts come to a fair conclusion based on evidence that we can provide thanks to the expertise of our cyber threat and dark web analysts and the insight we can provide into cybercriminal communities and tactics.

Can the stolen data be used to commit identity theft?

One of the critical determinants of a class action lawsuit hinges on the type of data that has been stolen and whether it can be used on its own to commit identity theft. In this sense, all data breaches are not quite the same.

When data is stolen, if it has any value at all to fraudsters, it usually turns up on dark web marketplaces, where it is clear that pieces of personal data have differing value to cybercriminals.
Opening bank accounts, making purchases, or claiming benefits based on someone else's identity requires specific privileged information. We can make precise determinations on what information is necessary to commit specific criminal schemes and we are able to comment to the contrary when data breaches do not contain sufficient PII to advance fraudulent activities.

Dark websites that cater to identity thieves usually carry inventory that focuses on the types of data required to commit financial fraud. In the cybercriminal world these data packages are referred to as a 'Fullz'. Fullz, at a minimum, includes the victim's full name and billing address, credit card number, expiration date and card security code, as well as their social security/national insurance number and birth date.

Risk exposure on the dark web

Another aspect we are often asked to investigate as part of class action work is the level of exposure those affected by the breach already have on the dark web. The rationale for this is to establish whether the breach in question has genuinely increased individual identity or financial fraud risk.

It often comes as a surprise when people learn just how much of their data is already available on the dark web. Our dark web analysts conduct exhaustive searches of deep/dark web sources to establish what personally identifiable information is obtainable and identify the historical breaches from which it originates.

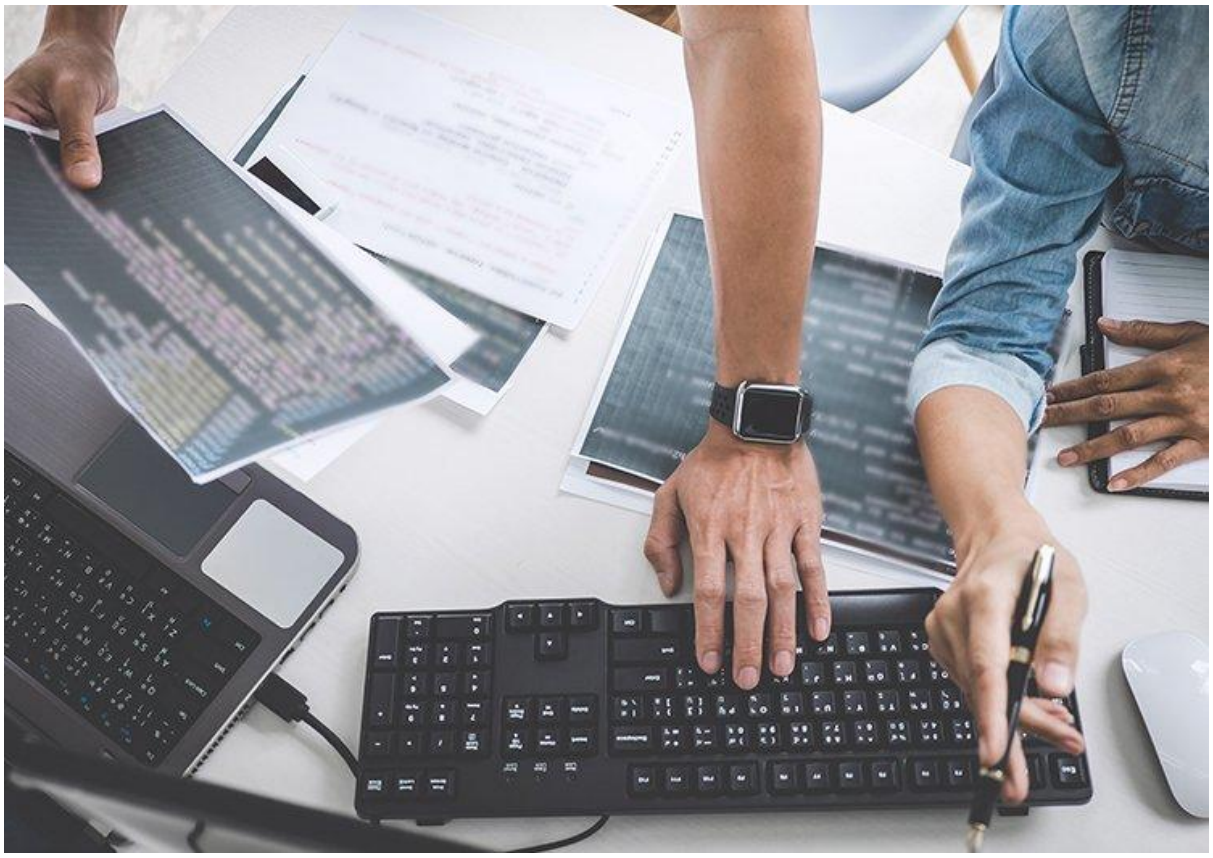
We can build a full picture of an individual's presence online. This could include lists of stolen account log-in and password details, as well as PII such as driver's


IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

license information, residential history, and social security data. If class action participants had low exposure prior to the breach at issue, their claim that the breach has raised their risk can be validated. If, however, much of their personal data was already available, their position – in the case of this specific breach – is, potentially, not as strong.

Assembling this evidence requires support from an authoritative and credible expert witness with covert presence on the dark web from which to conduct investigations, such as the presence we maintain at BlueVoyant. Our analysts, who have honed their craft in international intelligence agencies and at the highest levels of private sector cyber intelligence, can build this portfolio of information to lend evidence-based clarity and substance to legal arguments.



What can individuals do to protect their data?

Experience tells us that it's vital individuals keep high-value personal data under tight control so that, in the event of a breach, your risk of identity theft or financial fraud can be reduced. This means keeping social security/national insurance numbers, credit card information and PII closely guarded, for when combined they can be the prime tools for identity verification by financial and government institutions.

IT for CEOs & CFOs is published by House of Words Media Limited.

The current issue and full text archive of this journal is available on **https://www.itceoscfos.com**

Also, the importance of account password hygiene cannot be overstated. Cybercriminals who buy a list of names, emails and passwords exfiltrated from a breach at one organization will try them out with other businesses, meaning if you use the same log-in details with your favourite clothing store as you do for your bank, a breach of one of them compromises your security with the others.

Ultimately, no one wants to be involved in a data breach class action but, when they do happen, understanding the value of the data stolen, whether it has surfaced on the dark web, and the level of victims' existing exposure are the key factors the court needs to use to reach its verdict. That is where we can help. At BlueVoyant, we can research, analyze, and present evidence that helps courts to reach a fair conclusion in data breach class action lawsuits.