Sep 19 2017 at 12:15 AM | Updated Sep 19 2017 at 12:15 AM

Equifax data breach a wake-up call for investors

Hackers were able to access Equifax data between mid-May and July 2017 due to a vulnerability in web application software. **AP**

by **Stirling Larkin**

It is not easy to rattle billionaires and those in the ultra-high net worth investment community, but the data breach by credit-rating company Equifax on September 7 did exactly that.

Coupled with the recent Bluetooth technology threat posed by the "BlueBorne" virus, a plethora of other cyber security infractions, questions surrounding the bona fides of Bitcoin and the lauded blockchain technology sitting behind it, and the sudden increase in what is being dubbed Virtual Family Office, or VFO, services, UHNW investors are rightfully concerned.

These threats exact a clear and present danger to all investors, but UHNW investors feel more exposed simply because of the larger quantum of savings involved and the broader disbursement of them across different geographies, platforms and currencies.

On September 7, Equifax disclosed a data breach that impacts 143 million American customers, with compromised data including names, social security numbers, and other sensitive information.

Hackers were able to get access to Equifax data between mid-May and July 2017 due to a vulnerability in web application software. Some 209,000 credit card consumers were compromised and 182,000 consumers had dispute documents with personal identifying information hacked as well.

Worse still, Equifax disclosed unauthorised access for certain UK and Canadian residents, but did not disclose the scope of the breach.

Given that Equifax acquired Australia's Veda in 2016, it would not come as a surprise to learn that Australian residents were also caught up in these breaches.

But for Australian UHNW investors this distinction is almost arbitrary because many Australian private bank and global wealth management providers hold custody of their clients' wealth in US dollars, US domiciled or US facilitated jurisdictions, all of which could have easily been caught up in this breach.

For other Australian investment communities thinking they side-stepped a bullet, they may wish to take pause and remember that Australian quoted exchange traded funds, which have an underlying exposure of more than $US64,000 may indeed have been reported to the US SEC regulator, given cross-border quotation reporting requirements of the ETF issuers. It is unclear whether such information was compromised in the September breach.

Related Articles

Rate rises to trigger $1.6trn debt bomb

US launches criminal probe into Equifax

Chemist Warehouse is a gold mine

Separating the dos from the don'ts of investing

Disruptors fast track home loans

Latest Stories

Malcolm Roberts' email fail
2 min ago

Crown slashes executive pay
10 mins ago

Markets Live: ASX tumbles after Fed
LIVE

More

Australia exposed

Highlighting these examples serves to remind Australian investors that even though international cyber infractions may not directly affect them, given the globalised nature of wealth management in the modern era, we may all be inadvertently exposed and should take all threats seriously.

The Equifax breach stands out not only because of the number of consumers impacted – 143 million consumers compared to 41 million in the December 2013 Target breach, although lagging the 500 million-1 billion in the Yahoo breaches – but because of the high degree of sensitivity of data exposed. The nature and magnitude of this attack will keep security software top of mind for family offices' chief investment officers at a time when regulation is getting stricter.

It was noted by analysts that if the Equifax breach had been subject to Europe's May 2018 general data protection regulation (GDPR), Equifax may have faced approximately $US65 million in fines.

Australian UHNW investors and their family office representatives are equally concerned about the ascending popularity of blockchain, given that its likely to be rolled out across not only international banking platforms but Australian domestic bank clearing facilities as well.

According to Professor Robert Faff, director of research at the University Queensland Business School, "Blockchain is heaped in mystique and opacity. Whether well founded or not, it has many of the hallmarks of notorious schemes throughout history. Until the bone fides are properly verified and better understood, I would urge caution by all, from regulators, to banks, financial markets and especially those most vulnerable – households."

Such sentiments were echoed earlier this week by JPMorgan Chase chief Jamie Dimon, who referred to Bitcoin as a "fraud".

This all coincides during a time when affluent Australian families are being asked to consider VFO services, which shift the emphasis from brick-and-mortar offices and facilities, to those found virtually, via the cloud and the internet.

The central sales pitch for considering VFOs is that they purportedly deliver better investment, tax, legal, investment banking and consulting services at a fraction of the cost of owning and operating one's own single family office, or "SFO".

Many affluent Australian families rightfully remain cautious and dubious about this proposition.

Following a year when it is alleged that the US presidential election campaigns were compromised by a cyber breach of the US Democratic National Congress by Russian proxies and intellectual property theft accusations continue to cross the Pacific between China and the US, the issue of cyber security for both individuals and entire economies becomes paramount.

The Equifax breach, albeit alarming, may be a well-timed wake-up call for Australian investors, prompting them to take a more serious look over their current digital footprints.

Stirling Larkin is chief investment officer of Australian Standfirst
australianstandfirst.com

AFR Contributor

Australia's hottest new export

What to wear in Melbourne at twilight

Why Melania Trump loves Delpozo

The designers making money from 3D fashion

The best place to be a jewellery maker

Stop the meeting madness

MBA Rankings 2017: The best MBA courses in Australia

Google's diversity dilemma

Short, fast and intense courses for busy executives

University of Sydney Business School tops BOSS 2017 MBA rankings

True romance with an unusual jeweller

2017 World Heritage sites for your bucket list

Love 'em or loathe 'em, bike helmets could do better

Sheep commodes and other collectable furniture

To look powerful, embrace this latest fashion trend

Special Reports

Uplifting education the goal

Taking Australian universities to the world

Why 'old school' methods should not be forgotten

STEM critical, but not the sole solution

Transforming the workforce

The Australian Financial Review
www.afr.com

SUBSCRIBE LOG IN

Subscription Terms
Digital Subscription Terms
Newspaper Subscription Terms
Corporate Subscriptions

Contact & Feedback
About us
Our Events
FAQ
Contact us
Letters to the Editor
Give feedback
Advertise
Site Map
Accessibility

Markets Data
Markets Overview
World Equities
Commodities
Currencies
Derivatives
Interest Rates
Share Tables

Brands
The Australian Financial Review Magazine
BOSS
AFR Lists
Chanticleer
Luxury
Rear Window
The Sophisticated Traveller

Fairfax Network
The Sydney Morning Herald
The Age
Adzuna
Domain
Drive
RSVP
Essential Baby
Home Price Guide
Weatherzone
Oneflare
The Store

Reprints & Permissions Privacy Policy Terms & Conditions of Use