KEEPER | PRESS RELEASE

A Brexit and Covid double whammy leave UK financial services companies vulnerable to cyberattacks

London, UK, 19 January 2021 – Consumed by emergencies stemming from Covid-19 and Brexit, the UK finance sector has failed to keep cybersecurity front of mind - with disastrous consequences. Some 70% of UK financial firms suffered a cyberattack in 2020 and 59% of these attacks were exacerbated by conditions forced upon them by Covid-19, according to new research by the Ponemon Institute and commissioned by Keeper Security.

The mass shift to working away from the office has provided a prime opportunity for cyberattackers to access sensitive information in remote environments. In fact, over half (57%) of companies in the UK finance sector believe cyberattacks are increasing in severity as a result of their staff operating in remote environments. Additionally, 41% finance bosses feel remote workers are putting the business at risk of a major data breach.

Worryingly, the increased use of personal devices by employees, often without sufficient guidance, means sensitive information is being accessed using platforms unprotected by enterprise security infrastructure. The use of personal devices has left much of the finance industry feeling vulnerable to attack, with 70% claiming their use has hindered business security. Despite this, half (50%) of UK finance companies say they still don't have adequate cyber-incident response plans in place.

"The adjustments to life as we know it due to Covid-19, and the limitations set to be imposed by Brexit, have seen businesses struggle adopt essential operational requirements to stay afloat," explains Darren Guccione, CEO and Co-founder of Keeper Security. "The UK finance industry needs to be especially cautious, given that the wealth of data it possesses is lucrative for cyberattackers on the dark web. With the pandemic already throwing the sector into disarray, business leaders need to act fast and take their online security seriously."

In particular, Guccione believes a stronger stance is needed within the finance sector around passwords to ensure all devices within the organisation are secure. A reliable security infrastructure is more crucial than ever as UK financial service providers battle for business without current access to the EU's single market for the services industry in the wake of Brexit.

"If they do not, 2021 and beyond looks bleak. Without rigorous security in place, financial institutions across the UK jeopardise their future. It only takes one cyberattack to destroy the reputation of the entire business. Since passwords are the most common avenue of attack for cybercriminals, investing in an advanced, encrypted solution that safeguards user credentials can be an easy, yet highly effective first step for financial institutions wanting to adequately protect themselves. The time for financial companies to take swift action and invest in cybersecurity is contracting," warns Guccione.

About Keeper Security, Inc.

Keeper Security, Inc. (Keeper) is the highly-rated and patented cybersecurity platform for preventing password-related data breaches and cyberthreats. Keeper's zero-knowledge security and encryption software is trusted by millions of people and thousands of businesses across the globe to mitigate the risk of cybertheft, boost employee productivity and meet compliance standards. Keeper has been named PC Magazine's Best Password Manager of the Year & Editors' Choice, PCWorld's Editors' Choice and is the winner of four G2 Best Software Awards and the InfoSec Award for Best Product in Password Management for SMB Cybersecurity. Keeper is SOC-2 and ISO 27001 Certified and is also listed for use by the U.S. federal government through the System for Award Management (SAM). Learn more at **keepersecurity.com**.