New Kill-Pill and Device Management Features Allow LogMeOnce Users to Manage, Track and Wipe Data from Lost Devices

LogMeOnce also adds BYOD support to improve productivity and enable employees to securely access corporate apps from personal devices

Washington D.C. – July 20, 2016 – LogMeOnce, the innovative leader of identity and password management in cloud and mobile enterprise, today announces three new features making it simpler to manage, track and wipe personal and business data from the LogMeOnce app on lost or stolen devices. LogMeOnce's Kill-Pill and Mobile Device Management (MDM) features enable individuals, businesses and IT administrators to easily enroll and manage devices, verify compliance and even wipe data stored in LogMeOnce if necessary. Additionally, LogMeOnce BYOD, or bring your own device, enhances office productivity and security of sensitive data by giving employees the ability to use their personal devices at work while keeping LogMeOnce data for personal and business use in separate vaults.

"70 million smartphones are lost each year according to a study from Kensington, so it's important you're protected in case it happens to you," says Kevin Shahbazi, CEO of LogMeOnce. "Losing your phone gives hackers free range to any data you store on the phone, from banking information to sensitive company documents. This not only has implications on you personally, but it puts your company at risk for a hack too. LogMeOnce Photo*Login* already provides several options for secure login and by adding the new Kill-Pill feature, we are making it easy to protect LogMeOnce data on a lost or stolen device."

LogMeOnce is introducing the following features for consumers using its Ultimate edition and organizations using either the Business or Enterprise editions:

Kill-Pill is a remote device wipe for when your phone or tablet is lost or stolen. To send a Kill-Pill to your mobile device, simply log into your LogMeOnce account on a desktop, and send the Kill-Pill to the lost device to wipe the vault and access to the LogMeOnce app itself on the missing device. Initiating Kill-Pill on a lost device ensures that a hacker or thief who may have your device is unable to login and access your data.

Mobile Device Management enables you to optimize the functionality and security of mobile devices in your family or within the enterprise**.** When MDM is enabled, you can see the device name, the last time it was accessed, geolocation, a comprehensive status about its operation, updates status, CPU, device identifiers and have the ability to initiate comprehensive remote commands including a ring tone to hear if the device is nearby. It can securely manage and retire mobile devices while allowing individuals and businesses to easily add or retire devices, for other users or for themselves. It eliminates any uncertainty of where your device is by allowing users to remotely locate lost or stolen devices from their LogMeOnce account.

LogMeOnce's BYOD feature is an IT feature policy that allows employees to use their personal mobile devices to access an organization's protected business vaults. Companies can also implement BYOD policies to extend business apps to their team members to increase productivity and prevent security threats. Employees can keep LogMeOnce personal and business data separate by creating two different "vaults". The "personal vault" holds the employee's personal data, and business administrators can accept an outside device on the company network and create a separate "business vault" to store

business-related data only. For greater privacy and efficiency employers have no knowledge of what an employee does on their personal device or in their personal vault. Pre-registered devices are protected with LogMeOnce **Photo*Login***, paired with the user account and automatically configured with corporate connectivity, security settings and device-specific restrictions. If an employee parts from the company, data separation allows IT administrators to wipe the LogMeOnce business vault without erasing the user's personal vault.

The new LogMeOnce Kill-Pill, Device Management and BYOD updates are currently available on the browser extensions for Chrome, Firefox, Safari on Windows and Mac, as well as iOS and Android platforms. For more information about LogMeOnce, Kill-Pill, Device Management and BYOD, please visit www.LogMeOnce.com.

About LogMeOnce
Confidently helping consumers and organizations protect their identity, data and information with identity and access management solutions, LogMeOnce develops, markets and supports a seamless and secure Single Sign-On, Identity and Access Management productivity suite. As an Independent Software Vendor (ISV), LogMeOnce's security suite includes a wide range of products, productivity solutions, cryptographic and e-security applications. LogMeOnce markets and sells its solutions worldwide directly and through a variety of partners.

Media Contact
Lauren Jaeger
Uproar PR for LogMeOnce
ljaeger@uproarpr.com
312-878-4575 x 246