

## **IAITAM HEAD: DON'T BUY "SCAPEGOATING" BY FORMER EQUIFAX HEAD IN TESTIMONY TO CONGRESS**

***Equifax Was Not Failed by One Employee; Instead, the Company Let Down 145 Million Customers by Failing to Put Proper ITAM Systems and Controls in Place***

**CANTON, OHIO – October 4, 2017 –** When the former CEO of Equifax testified before Congress yesterday, he misled lawmakers and the American public by attempting to place the blame for the massive breach at the credit-reporting agency on one person, according to Dr. Barbara Rembiesa, president and CEO of the International Association of IT Asset Managers (IAITAM).

The truth, according to Dr. Rembiesa, is that Equifax failed as a company when it neglected to put standard Information Technology Asset Management (ITAM) systems and controls in place that would have prevented the breach. In an earlier statement on September 8<sup>th</sup>, IAITAM said that the Equifax's second major breach in four years was inexcusable and could have been avoided. See: <http://iaitam.org/iaitam-news-release-massive-equifax-data-breach-points-ongoing-u-s-corporate-failures-information-technology-asset-management-itam-use/>.

In a new statement issued today, Dr. Rembiesa said: "During his testimony before the House Energy and Commerce Committee, former Equifax CEO Richard Smith disclosed that it was a failure to upload a security patch for the Apache Struts systems that Equifax was using. The Department of Homeland Security's Computer Emergency Readiness Team (CERT) sent emails to several companies, including Equifax, which notified them about the vulnerabilities to the Apache Struts systems. This notice was sent on March 8<sup>th</sup>. While internal policy was to ensure that all systems were updated within 48 hours, this clearly did not happen. Everyone, from House Committees to innocent people who had their identities stolen, are left wondering why."

"According to Smith, it is a human error issue. A single individual is being scapegoated in this scenario. During the testimony, Smith stated that the employee who is responsible was identified and that it was 'human error' that caused 145 million identities to be stolen. However, this was not as simple as a human error as Smith has tried to make it seem." Dr. Rembiesa continued: "IT Asset Managers have a phrase for these very instances: Version Control."

"It is due diligence on the part of an IT Asset Manager and their ability to utilize discovery tools (the tools which pull software data from the organization's environment) that ensures proper versions of software are installed on organizational assets. This originally became a responsibility of an IT Asset Manager because software publishers began to charge organizations based on the software licenses they were running and which versions of software were supported by the organization. The unintended, but beneficial consequence to this development, was that IT Asset Managers were becoming instrumental in safeguarding and securing an organization and their data. Simply stated, it is people who run organizations through tools, not tools that run organizations through people."

“IT Asset Managers are responsible for an action called ‘Reconciling’. This job function ensures that the data being reported by discovery tools match what is required by the organization. It is by this action of reconciliation that an IT Asset Manager would have discovered that the version of software for the Apache Struts systems was not correct with the newest patch necessary to maintain data security. This risk would have been identified, mitigated, and fixed well before this breach occurred.”

Dr. Rembiesa concluded: “The excuse Smith has posed about the breach being a ‘human error’ is another way of saying that the proper people were not in place to ensure the safety and security of the data, or the people now exposed. The human error, was not having an IT Asset Manager.”

### **ABOUT IAITAM**

The International Association of Information Technology Asset Managers, Inc., is the professional association for individuals and organizations involved in any aspect of IT Asset Management, Software Asset Management (SAM), Hardware Asset Management, Mobile Asset Management, IT Asset Disposition and the lifecycle processes supporting IT Asset Management in organizations and industry across the globe. IAITAM certifications are the only IT Asset Management certifications that are recognized worldwide. For more information, visit [www.iaitam.org](http://www.iaitam.org), or the IAITAM mobile app on Google Play or the iTunes App Store.

**MEDIA CONTACT:** Alex Frank, (703) 276-3264 or [afrank@hastingsgroup.com](mailto:afrank@hastingsgroup.com).