

Addressing the Big 3: Compliance, Fraud & Cyber Security

What the NSA Whistleblower's Revelations Mean for Your Credit Union's Email Practices

While NSA surveillance whistleblower Edward Snowden has become something of a champion for libertarians around the world, the information he's disclosed is actually quite important for people of all ideologies.

Credit union professionals are one segment of people who will need to pay particular attention. A higher standard for data privacy is emerging in 2014, born of the public's awareness of data privacy vulnerabilities that the NSA and "less legitimate" parties can exploit.

The implications of this higher standard for email privacy are many – and they will directly influence your credit union's ability to maintain your members' trust and satisfaction.

Consider the following:

1. Public privacy concerns about the NSA email surveillance program have caused world-wide consumer awareness that standard email is not private;
2. When your members now receive their financial information, or social security/personal information in standard email from you, they are now aware that the information has not been transmitted in a private manner;
3. With a little research, your members will easily learn that there are regulations requiring you to transmit their financial information, or social security/personal information, in a secure, encrypted manner;
4. They may also find that there are certain whistleblower awards paid by the regulators to those that provide evidence of non-compliance with data privacy regulations; and
5. The evidence of non-compliance is already in their inbox – any standard email sent from you to them that is in their inbox containing their financial information, or social security/personal information.

In 2014, email encryption will emerge as a critical business process.

If you are currently using an email encryption service that uses a "store-and-forward" method of serving encrypted email content, there is a danger you need to be aware of. "Store and forward" email encryption services typically require recipients to register to download encrypted content – this constitutes a major inconvenience that is compelling your member service representatives to circumvent your compliance protocols or revert to more costly paper-and-courier mail delivery.

When NSA whistleblower Edward Snowden's initial revelations were made public, RPost prepared a detailed analysis as to what NSA surveillance means for email users; in terms of message privacy. We shared Snowden's disclosure that email encryption was one of the few things that actually worked [to prevent data breaches], though "endpoint security" could be seen as a vulnerability. In a follow-up analysis, we went on to discuss how RPost's email encryption service, unlike competitors' offerings, is particularly resistant to data breaches and how RPost upholds data security even at the endpoints.

Zafar Khan

Chairman & Chief Executive Officer



Zafar Khan is Founder & Chief Executive Officer of RPost and was identified by Citytech Magazine as among the top 100 global technology

leaders. He has strategy and finance experience with Braxton Associates/Deloitte Consulting and Goldman Sachs; and has been in the technology field for more than 10 years. He has worked to transfer U.S. Department of Energy National Lab weapons technology to industry and was one of 15 CEOs elected to participate in a U.S. Presidential Trade Mission. Khan has invented two U.S. patents, holds a Bachelor of Arts degree from Wesleyan University in Connecticut, an International Business Certificate from The Georgetown University School of Business, and a Master of Business Administration degree from The Wharton School at The University of Pennsylvania.

Contact Info

www.rpost.com

866-468-3315

For more information:

<http://www.rpost.com/cutechtalk>