Data Breach Considerations for CU Management

Working with Frontline Staff
Your frontline staff is just that ... your front line. While your legal and regulatory folks will certainly know more about the subject at hand, your tellers will be the ones fielding the first line of questions.

In this kit, we've also included tips and basic responses to common member questions. Consider using this sheet, modifying it or developing your own — then going over it with staff. Make sure you've worked on consistent answers to likely questions. Make sure the frontline staff knows where to direct members with more technical questions, and make sure they're not afraid to say "I'm not sure, but I'll work with management to get you an answer."

Reporting to Equifax
A common question we've heard from credit unions in the wake is this data breach is whether or not they should stop reporting member information to Equifax. There's not a good blanket response to this inquiry — it's a significant business decision your credit union will need to discuss with its board and legal counsel.

If you are considering ceasing reporting to Equifax, it's crucial that you find and review any and all Equifax contracts with legal counsel. Understand that should you stop reporting, member tradelines will remain with the credit bureau from previous reporting. In this case, your credit union will also need to identify and remove previously reported information.

Evaluating Safeguards
On the technology front, considering the following (if not already in place):

- Increasing security tokens to include out-of-band authentication (out-of-band authentication is the practice of requiring the user to make a phone call from a registered number or respond to an automatically-generated phone call or SMS text from the institution).
- Utilize multiple factor authentication
- Educate all staff members about social engineering and how this type of data can be used
- Review internal policies such as Red Flag Rules to ensure it addresses the most up-to-date tactics
- Post an advisory on your social channels for members

Communicating to all Parties
Though credit unions are not at fault, this clear and present danger poses liability concerns. MCUL advises all credit unions to communicate this issue loud and clear both internally and externally.

Again, make certain that all staff are speaking with a strategic, unified message. Make certain that this plan is communicated and agreed upon at all levels, including senior management and the credit union's board of directors, so that everyone is actively participating in resolution.

Make certain that the credit union's stance and response is clearly communicated online. For many members, especially millennials, your website and/or app is the primary means of credit union interaction.

Keeping Abreast of the Greater Landscape
Already, there are at least 4 lawsuits which will surely lead to class-action proceedings. Again, confer with legal counsel and know your options.

Additionally, multiple congressional committee are looking at the issue. Chairman Hensarling (House Committee on Financial Services) has indicated that he'll hold hearings. We expect the Senate Banking Committee to hold hearings, and we shouldn't be surprised if the Judiciary Committee gets involved. This may finally spur action on data breach legislation. Make sure your credit union ready to contact state and federal lawmakers when MCUL and CUNA put out a request.

For more information, watch the recorded CUNA & FS-ISAC Fraud Mitigation Post-Data Breach Webinar here.