Concerning the Equifax Breach

Dear Valued Customer,

If you have not already heard, we want you to be aware that Equifax, one of our key credit bureau partners, was victim to a cybersecurity incident in May and July 2017. We wanted to provide you with additional information and make you aware that there was no additional harm incurred as a client to Ser Technology.

Equifax has made it clear to us that there was no evidence of unauthorized access to the core Consumer or Commercial Credit Reporting databases that Ser products screen against. The intrusion occurred to a separate income verification database.

A select set of our products do screen against the Equifax credit reporting databases for prescreen, trigger or account review output. **The databases that are used for our products are not amongst those affected by the breach. Further any input or output files that are provided or received by Ser specific to your credit union were not exposed.**

We consider this issue the highest priority. While the breach did cause the exposure of sensitive data for the broader population, **credit unions and their members would not have been any more adversely affected as a client of Ser Technology.** A set of Equifax's data was exposed, but the impact of the breach would be equivalent to any consumer or credit union irrespective of their status as a Ser client.

The greatest potential impact of the breach is 143 million U.S. consumers; however, Equifax continues to investigate the actual number of consumers affected for which they expect to be a lower amount. We understand that the vulnerability which resulted in a breach has been addressed.

While our clients were not any more adversely affected by this breach, we want you to understand what information Ser does send and receive from the credit bureaus.

- Our input file that Ser exports to Equifax contains the bare essential information needed to identify the member to be matched in the credit database: name, address, city, state and zip.

- Non-public information covered by Gramm-Leach-Bliley is not included in the export, including fields such as account number, social security number, birthdate and phone number.

- The prescreen output file returned to us by Equifax contains no identifying field heading information indicating what the data is. If a file was ever compromised, the file itself does not assist the thief to understand the content.

- The output file is an undocumented fixed record format such that it is difficult or impossible to differentiate one field from another, upon visual inspection.

- No credit union is identified by name within the data. Credit unions' identity is an integer value assigned by Ser and meaningful only to Ser.

We will continue to monitor with Equifax and will keep you informed of any new information.

Below is a section of the Equifax press release providing information to consumers about (i) determining whether they were affected and (ii) offered services if they were indeed affected.

We value you as a customer, and we treat such sensitive information with the greatest care and attention. We are always available to speak further as you would like to.

Sincerely,

James Lee
Chief Operating Officer
Ser Technology Corporation
469.941.5112
james.lee@sertech.com

Excerpt from: *Equifax Announces Cybersecurity Incident Involving Consumer Information*
September 7, 2017

Equifax has established a dedicated website, www.equifaxsecurity2017.com, to help consumers determine if their information has been potentially impacted and to sign up for credit file monitoring and identity theft protection. The offering, called TrustedID Premier, includes 3-Bureau credit monitoring of Equifax, Experian and TransUnion credit reports; copies of Equifax credit reports; the ability to lock and unlock Equifax credit reports; identity theft insurance; and Internet scanning for Social Security numbers - all complimentary to U.S. consumers for one year. The website also provides additional information on steps consumers can take to protect their personal information. Equifax recommends that consumers with additional questions visit www.equifaxsecurity2017.comor contact a dedicated call center at 866-447-7559, which the company set up to assist consumers. The call center is open every day (including weekends) from 7:00 a.m. – 1:00 a.m. Eastern time.

In addition to the website, Equifax will send direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were impacted. Equifax also is in the process of contacting U.S. state and federal regulators and has sent written notifications to all U.S. state attorneys general, which includes Equifax contact information for regulator inquiries.

Equifax has engaged a leading, independent cybersecurity firm to conduct an assessment and provide recommendations on steps that can be taken to help prevent this type of incident from happening again.