Exhibit A

25

Subject: Objection to Class Settlement - Insufficient Compensation for Stolen Medical Data

Cyril Stark
30 Revere Beach Pkwy, apt 704
Medford, MA 02155
cyrilstark@gmail.com
617.653.3237

December 17, 2023

Hon. Janice W. Howe
Superior Court Justice
Superior Court - Essex
56 Federal St.
Salem, MA 01970

Re: LaFratta v. Medical Healthcare Solutions, Inc.
Case No. 2277CV00106 C

Dear Honorable Janice W. Howe,

I am writing to formally object to the proposed class settlement in the matter referenced above. I am a member of the affected class, and my name is Cyril Stark. I appreciate the court's attention to this matter and the efforts made to address the unauthorized access and theft of sensitive medical data.

While I recognize the complexity of assessing damages in cases of data breaches, I must express my concern that the proposed settlement of $50 per affected individual is inadequate given the potential ramifications of the compromised information. The stolen medical data, which includes deeply personal and sensitive details, has the potential to cause significant harm that extends far beyond any immediate financial losses.

Medical information is inherently private, and its exposure can have far-reaching consequences, particularly in an era where decision-making processes are increasingly driven by algorithms. The potential integration of this stolen data into financial and employment systems poses a direct threat to individuals' opportunities and well-being.

Consider for example the scenario where an affected individual has a medical diagnosis for depression. The use of this information in the decision-making processes of banks or employers could unfairly disadvantage the affected individual in, e.g., mortgage or job applications. The latent impact on various aspects of life, both personal and professional, cannot be accurately quantified at this stage. That's because neither the flow of said information online as well as the power of future data analysis algorithms is unknown.

While I don't believe that the stolen data will be used directly by a bank to evaluate a mortgage application by an affected individual, the bank or the employer may work with external companies to help them evaluate mortgage or job applications. These external companies build datasets about individuals where the stolen medical data may appear in clear-text or (more likely) in codified form.

The proposed settlement of $50 per affected individual fails to reflect the gravity of the situation and does not adequately compensate for the potential harm and ongoing risks associated with the breach. To compensate for this, to deter future negligence, and to underscore the importance of robust data protection measures, I ask the court to reconsider the settlement amount.

I believe it is crucial for the penalty imposed on the responsible party to be commensurate with the potential long-term consequences of their actions. A more substantial settlement would not only provide just compensation to the affected individuals but also serve as a deterrent for other companies, emphasizing the imperative to safeguard sensitive data.

Ideally, legal action could also be taken against companies that work with Medical Healthcare Solutions, Inc. That's because they have failed to adequately check that the companies they share sensitive data with have the ability to protect sensitive data.

In conclusion, I respectfully request that the court reconsiders the proposed settlement amount, taking into account the severity of the breach and the potential harm inflicted on impacted individuals. Your thoughtful consideration of these concerns is greatly appreciated.

Thank you for your attention to this matter.

Sincerely,
C. Stark
Cyril Stark