IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

DAVID MUTNICK, for himself and others similarly situated,	)	
	)	Case No. 20 C 512
Plaintiff,	)	Judge Sharon Johnson Coleman
v.	)	Magistrate Judge Maria Valdez
CLEARVIEW AI, INC., *et al.*	)	
Defendants.	)	

PLAINTIFF'S NOTICE OF SUPPLEMENTAL FACTUAL INFORMATION IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION

Plaintiff David Mutnick, through his attorneys, respectfully notifies the Court that on April 16, 2020, it was disclosed that Defendant Clearview AI, Inc. ("Clearview") recently experienced another serious data security breach, providing further grounds for Plaintiff's requested preliminary injunction (Dkt. 31-32). In his preliminary injunction motion, Plaintiff Mutnick predicted that "given Defendants' lack of concern for data security and their new-found notoriety, it is extremely likely that Defendants will experience additional and more severe data breaches, further injuring those whose data they wrongfully acquired in the first place." Dkt. 32 at 13. He was right.

According to Tech Crunch – a top online source for breaking technology news – a cybersecurity expert recently revealed that Defendant Clearview had a "misconfigured server" that "exposed the company's internal files, apps and source code for anyone on the internet to find." Exhibit 1 at 1.[1] As a result of the security breach, anyone could run Defendant Clearview's

[1] Zack Whittaker, *Security Lapse Exposed Clearview AI Source Code*, Tech Crunch (Apr. 16, 2020), https://techcrunch.com/2020/04/16/clearview-source-code-lapse/ (last accessed on Apr. 16, 2020).

application software and access its biometric database that contained the biometric identifiers and information of over 3 billion individuals, including Plaintiff and Class Members. *See id.* at 1-2. Moreover, the security breach revealed that Defendant Clearview's server had 70,000 videos of a lobby in a residential building that showed residents entering and leaving the building. *Id.* at 3.

Upon being confronted about the security breach, Defendant Hoan Ton-That conceded that Defendant Clearview "'experienced a constant stream of cyber intrusion attempts . . . .'" *Id.* at 2. While Defendant Ton That contended that Defendant Clearview was investing in increased security, Tech Crunch reported that Defendants sought to conceal the security breach at issue by offering to pay the cybersecurity expert in return for a nondisclosure agreement. *See id*. at 2-3.

Based on Defendant Ton-That's above-described statement and Defendant Clearview's attempt to conceal the security breach, it is clear that the biometric identifiers and information of Plaintiff and Class Members that Defendants unlawfully collected and possess are not safe or secure. Accordingly, the Court should grant Plaintiff the requested preliminary injunction which seeks, among other things, that the Court preclude Defendants from continuing to possess the biometric identifiers and information of Illinois residents without taking adequate and reasonable measures to ensure the security of the identifiers and information.

Dated: April 17, 2020

Respectfully submitted,

/s/ Scott R. Drury
SCOTT R. DRURY

Arthur Loevy (arthur@loevy.com)
Michael Kanovitz (mike@loevy.com)
Jon Loevy (jon@loevy.com)
Scott R. Drury (drury@loevy.com
LOEVY & LOEVY
311 N. Aberdeen, 3rd Floor
Chicago, Illinois 60607
312.243.5900

CERTIFICATE OF SERVICE

I, Scott R. Drury, an attorney, hereby certify that, on April 17, 2020, I filed the foregoing document using the Court's CM/ECF system, which effected service on all counsel of record.

/s/ Scott R. Drury
One of David Mutnick's Attorneys