IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

AUTHENTICOM, INC.,

Plaintiff,

v.

CDK GLOBAL, LLC and
THE REYNOLDS AND REYNOLDS COMPANY,

Defendants.

ORDER FOR
PRELIMINARY INJUNCTION
AGAINST REYNOLDS

17-cv-318-jdp

Based on the parties' written submissions, documentary evidence, and the evidence presented at an evidentiary hearing, the court concluded that Authenticom is entitled to a preliminary injunction. Dkt. 172. As explained more fully in the court's July 14, 2017 opinion and order, (1) Authenticom has made the requisite showing of likelihood of success on the merits of its antitrust claims; (2) Authenticom will suffer irreparable harm if the court did not grant preliminary relief; (3) the balance of hardships tips in Authenticom's favor; and (4) the public interest is not disserved by the entry of a preliminary injunction. Accordingly, defendant the Reynolds and Reynolds Company is preliminarily enjoined as provided in this order. Those enjoined include defendant the Reynolds and Reynolds Company and its officers, employees, agents, attorneys, and all those acting in active concert or participation with them, which the court will refer to collectively as Reynolds.

Reynolds is preliminarily enjoined as follows:

1. Reynolds must not prevent Authenticom from using dealer login credentials to provide data integration services for dealers who, as of May 1, 2017, had authorized Authenticom to provide data integration services. Reynolds must

establish and maintain login credentials for its DMS for Authenticom, subject to the following conditions:

a. Authenticom may access only the parts of the Reynolds DMS that an authorizing dealer itself is authorized to access.

b. Authenticom may access and extract only the data fields that the dealer authorizes Authenticom to access and that are reasonably necessary for Authenticom to provide the data integration services that the dealer requests.

c. Authenticom's access to the Reynolds DMS is limited to read-only data exporting.

d. This order does not prevent Reynolds from blocking Authenticom's access to the Reynolds DMS that exceeds the access authorized in this order.

2. This order will be implemented through the following procedure:

a. Authenticom will request that each Reynolds dealer that intends to use Authenticom for data integration services during the pendency of this preliminary injunction sign a dealer authorization form. The dealer authorization form will authorize Reynolds to issue a single user ID to Authenticom for each dealer, created specifically for Authenticom to provide data integration services to that dealer and, in turn, to the various software vendors that provide services to that dealer.

b. The dealer authorization form must: be signed by an individual authorized to bind the dealer and to authorize the release of dealer data; identify the specific data fields within the DMS that the dealer authorizes Authenticom

to access; agree that the Authenticom-specific credentials will not be used by or shared with any person or entity other than Authenticom; and acknowledge that the dealer will not attempt to hold Reynolds responsible for misuse of the Authenticom-specific credentials or the data acquired with it. The dealer authorization form will also provide that the dealer authorizes Reynolds to suspend security measures directed specifically to blocking automated access for the Authenticom-specific credentials.

c. Reynolds must configure Authenticom's login credentials within five business days of receiving a dealer authorization form from Authenticom. If the volume of requests for configuration of Authenticom's credentials is such that Reynolds cannot reasonably meet the five-business-day deadline, Reynolds shall notify Authenticom and the parties shall work in good faith to determine a reasonable schedule.

d. Authenticom may not disclose its Reynolds credentials to anyone other than its employees who need to know them. Authenticom must adopt security measures to protect all user credentials associated with the Reynolds DMS. Such measures must include, but are not limited to, not transmitting credentials by unencrypted email.

e. Once Reynolds issues a username and password to Authenticom for a given dealer pursuant to this preliminary injunction, Authenticom will use only that username and password in providing data integration services for that dealer, and Reynolds may disable or block any other usernames or passwords Authenticom has used or uses for that dealer.

f. If a dealer receiving Authenticom's data integration services pursuant to this order elects to discontinue those services, Authenticom must promptly notify Reynolds in writing. Reynolds may then immediately disable the Authenticom-specific credentials for the terminated dealer.

g. For dealers that do not require more than one daily data refresh, Authenticom must access the Reynolds DMS for bulk-data queries between the hours of 10 p.m. and 6 a.m. (dealer local time).

h. When it provides a dealer authorization form to Reynolds, Authenticom must identify whether that dealer requires more than one daily data refresh. Authenticom must make all reasonable efforts to minimize the number of queries executed for those dealers during business hours.

3. If Reynolds detects either (1) a material security breach on its DMS that it believes, in good faith, is attributable to Authenticom's access to the DMS, or (2) the use of Authenticom's credentials by someone other than Authenticom, Reynolds may temporarily suspend the affected Authenticom-specific credentials. In the event of such a suspension, Reynolds must immediately notify Authenticom and promptly investigate the security event. If Reynolds does not restore or replace the affected credentials within 48 hours, it must explain in writing to Authenticom why it has not done so. This section does not limit Reynolds's ability to follow its standard security protocols if it experiences a security breach.

4. Reynolds may continue to perform normal or routine maintenance on its systems or to continue to implement standard security protocols (other than protocols that

prohibit automated access by Authenticom, as provided here), such as routine prompts for password changes.

5. Reynolds may comply with any request by any dealer to disable Authenticom's access to that dealer's data.

6. Reynolds may not enforce those provisions in its contracts with dealers or vendors that restrict, or have the effect of restricting, any dealer or vendor from obtaining data integration services from Authenticom. Such provisions include, for example, those that would require, or have the effect of requiring, a software vendor to obtain integration services exclusively from Reynolds for all of that vendor's applications or all of that vendor's dealer customers.

7. Reynolds may not retaliate against any dealer or vendor as result of its decision to do business with Authenticom, such as by terminating or blocking a vendor from the RCI program, or by imposing financial penalties, such as invoking liquidated damages clauses.

8. Within 10 business days of entry of this order, Authenticom must provide security in the amount of $1 million, in a form agreed to by the parties or approved by the court. This single $1 million bond will serve as security for both injunction orders issued in this case.

This order will take effect immediately and will remain in place until entry of final judgment in this matter or until the court orders otherwise.

Entered July 28, 2017.

BY THE COURT:

/s/

JAMES D. PETERSON
District Judge