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

AUTHENTICOM, INC.,

Plaintiff,

v.

OPINION & ORDER

CDK GLOBAL, LLC, and
THE REYNOLDS AND REYNOLDS COMPANY,

17-cv-318-jdp

Defendants.

This is an antitrust case involving the software used by car dealers. Defendants, CDK Global, LLC, and the Reynolds and Reynolds Company, are the main providers of comprehensive software packages called dealer management systems, which are used by virtually all United States car dealers. Plaintiff, Authenticom, Inc., is a third-party data integrator. It provides a service that links car dealers to third-party software vendors who provide features and enhancements that are not built into the dealers' DMSs. Authenticom contends that defendants have violated the Sherman Act in numerous ways, including by conspiring to drive it out of business. Authenticom seeks a preliminary injunction that would require defendants to allow Authenticom to continue its historical practice of accessing dealer data on defendants' information systems, using login credentials provided by dealers.

The case is complicated both factually and legally. But based on the parties' written submissions, documentary evidence, and the evidence presented at a two-and-one-half day hearing, the court concludes that Authenticom is entitled to a preliminary injunction. Authenticom's evidence establishes at least a moderate chance of success in proving that defendants have violated the Sherman Act. And the balance of harms tips sharply in favor of

Authenticom, because Authenticom is clearly at risk of going under without a preliminary injunction. The countervailing harm alleged by defendants—primarily the threat to the security of their information systems—is not persuasive because defendants already allow third-party access of the sort that Authenticom asks to continue. And there was no evidence that Authenticom itself had lax security practices or posed a specific threat to the security of defendants' systems.

FINDINGS OF FACT

I make no effort here to set out all the facts established by the parties' evidence or to review comprehensively that evidence. The parties have submitted declarations and documentary evidence, most of which is not objected to. Defendants have, however, lodged specific objections to a number of Authenticom's exhibits and some declaration testimony in Dkt. 171. For the most part, I will sustain defendants' objections.[1]

Focusing on the main points and issues, I find the following facts. Some additional facts are set out the analysis section.

A. Background

Virtually every dealer in the country uses a DMS, a dealer management system, to manage the major aspects of its business, from vehicle and parts inventory to service

[1] The newspaper accounts and other third-party documents are hearsay, and the objected-to declaration testimony lacks foundation. I will overrule the hearsay objection to PHX-009 and PHX-099, although I did not consider those exhibits in my decision. The only objected-to documents that I did consider are PHX-156 and PHX-159, which relate to the exceptions accorded to Penske dealers. I overrule the hearsay objection to these documents; ultimately defense witnesses conceded the existence of the Penske exceptions. I also overrule the objections to PHX-150 and PHX-151, although I did not consider these documents.

appointments to payroll. Defendants, CDK Global, LLC, and the Reynolds and Reynolds Company, provide and maintain the two most-used DMSs. Together, defendants provide DMSs to roughly three-quarters of the dealers in the United States. Dozens of other DMS providers serve the remaining quarter of the market, although Dealertrack appears to be the leading alternative to defendants' systems. Defendants provide the DMS software to the dealer and run the servers that hold the dealer's data. The data itself belongs to the dealer. Sophisticated DMS software, like defendants', is expensive. A dealer typically pays $8-10,000 per month for its DMS.

Dealers also use software applications from third-party vendors to provide features and services that are not built into the basic DMS, although these applications require data from the DMS. A typical dealer uses 10 to 15 vendor-provided applications in addition to its DMS. For example, a dealer might engage Carfax to provide a vehicle history report for every used car that it offers for sale. Somehow the dealer must get data about its inventory to Carfax, so that Carfax can provide the required reports. Generally speaking, dealers find it cumbersome to retrieve their own data from their DMS and send it to vendors, so most dealers authorize vendors to get the data from the DMS, either directly or through a third-party data integrator.

B. Authenticom

Plaintiff Authenticom, Inc., is a third-party data integrator, founded by Steve Cottrell in 2002. With the dealer's consent, Authenticom accesses the dealer's data on its DMS, downloads the necessary data, reformats the data to suit the needs of the vendor, and then sends the reformatted data to the vendor. The vendor uses the data to provide its services to the dealer. The dealer pays the vendor for its services, and the vendor pays Authenticom for its

data integration. Typically, a vendor pays Authenticom about $50 per month for each dealer for which data is provided.

In 2014, Authenticom introduced its DealerVault software. DealerVault provides an interface that allows dealers to monitor and control the data provided from its DMS to the vendors it uses. DealerVault is popular with dealers, who generally feel strongly that because they own their data, they should be able to control and monitor its use. Cottrell estimates that approximately 15,000 of 18,000 dealers nationwide have at one time or another relied on Authenticom for services. Dkt. 164, at 89:7-11.

The method Authenticom uses to acquire dealer data is a point of contention. Dealers who want to work with Authenticom provide Authenticom a username and password, which Authenticom uses to log into the dealer's DMS account on defendants' systems. Authenticom "screen scrapes" the data by capturing what is displayed, and then it cleans up the data to keep the needed elements. Authenticom works with a very large number of dealers, so it has automated this process. Authenticom's information systems are programmed to automatically and regularly log into dealer DMS accounts so that the data that vendors use is up to date.

The evidence generally shows that Authenticom is secure. DealerVault is hosted on Microsoft Azure, secure cloud technology. And the data to which Authenticom has access is controlled by the dealer. Wayne Fitkin, a veteran in the automotive IT industry and currently IT director for a dealership group, testified that although Fitkin himself has access to a large amount of extremely sensitive information, he creates a user ID specifically for Authenticom that has access to limited accounts and a single function necessary to query and scrape the

system. Dkt. 165, at 9:12-21. The court did not receive any evidence that Authenticom has ever suffered a security breach or that it has caused a security breach at another entity.[2]

C. Defendants block Authenticom

Defendants object to Authenticom's screen-scraping data extraction method, which they call "hostile access." Reynolds has never approved of third-party access based solely on the *dealer's* authorization. Reynolds allows third-party access only with its own approval, and preferably via an interface specifically designed for that purpose, the Reynolds Certified Interface (RCI). Through RCI, third parties—vendors, typically—access and receive specified data fields in a highly controlled environment. Reynolds contends that access via RCI is more secure and less burdensome on the Reynolds system than Authenticom's screen-scraping technique. The court accepts this point as a general principle, but Reynolds did not provide evidence to quantify the relative burden Authenticom places on the system, and Reynolds did not adduce any evidence of any actual or realized security threat attributable to Authenticom.

Reynolds began blocking Authenticom's access to its DMS in 2009, and it achieved more effective blocking around 2013, apparently by using technology that was able to detect and instantly disconnect automated access to its DMS. Reynolds' more effective blocking had a significant impact on Authenticom's revenue, because blocking interfered with Authenticom's ability to integrate data for vendors who served dealers using Reynolds' DMS.

Unlike Reynolds, until 2015, CDK offered what the parties and the court have been calling an "open system." An open system allows third-party integrators, such as Authenticom,

[2] In the time Authenticom has been in operation, there has been only one reported incident with defendants: several years ago, a faulty code placed by Authenticom caused the Reynolds system to cyclically reprocess the same code.

to access and scrape data from the DMS with dealer authorization. Indeed, until recently, CDK touted its open system as one of the competitive advantages of its DMS. In fact, CDK itself owned and operated third-party integrators, DMI and Integralink. Apparently the open system was appealing to dealers, as Reynolds' market share declined from approximately 40 percent to approximately 28 percent as CDK marketed its open system and Reynolds solidified its closed one. *Id.* at 84:7-17. CDK picked up most of the dealers who left Reynolds.

But things changed around 2014, as CDK reconsidered its third-party access programs. Internal documents and testimony from CDK witnesses suggest that two primary concerns motivated CDK's reconsideration. First, well-publicized security breaches prompted CDK to improve its cybersecurity, and CDK implemented a "Security First" initiative. (Notably, the Security First initiative recommended improved third-party access practices and retiring "certain integration that risks data integrity", but it did not specifically recommend terminating all third-party access. DHX-27.) Second, CDK realized that it was not getting all the value it could from 3PA, its third-party access program which is, essentially, the equivalent of Reynolds' RCI. So, after years of touting the benefits of its open system, CDK decided to bring data integration in house and transition toward a closed system.

D. The defendants' agreements

CDK's transition to a closed system roughly coincided with CDK and Reynolds signing written agreements in February 2015. The first of the three agreements was a so-called Data Exchange Agreement. Dkt. 106-1. In the Data Exchange Agreement, CDK agreed to wind down certain aspects of DMI, CDK's third-party integrator—specifically, those aspects that involved "hostilely integrating" with the Reynolds system. Reynolds agreed that it would not block DMI's access to the Reynolds system during the wind-down period, which might last as long

as five years. And CDK agreed to cooperate with Reynolds to have DMI clients—vendors using DMI to poll data from the Reynolds system—transition to RCI, Reynolds' in-house "data integrator." *Id.* §§ 4.1, 4.4. Defendants further agreed that they would not assist any person that attempts to access or integrate with the other party's DMS. *Id.* § 4.5. This section is described as "not intended as a 'covenant not to compete,' but rather as a contractual restriction of access and attempted access intended to protect the operational and data security integrity of the Reynolds DMS and the CDK DMS." *Id.* Section 4.5's terms do not expire. *Id.* § 6.1.

The remaining agreements in the set—the 3PA Agreement and the RCI Agreement—granted reciprocal access to defendants' in-house data integration platforms. Both Reynolds and CDK provide add-on software applications for dealers, just like third-party vendors. CDK wanted access to the Reynolds DMS for its applications, and Reynolds wanted access to the CDK DMS for its applications. *Id.* at 2. Under the agreements, CDK's applications could access the Reynolds DMS via RCI, and vice versa. Reynolds received five free years of 3PA access, purportedly as consideration for its allowing DMI's access to the Reynolds system during the wind down. By signing up for 3PA, Reynolds agreed that it would access the CDK DMS exclusively through 3PA, and Reynolds agreed that it would not "otherwise access, retrieve, license, or otherwise transfer any data from or to a CDK System (including, without limitation, pursuant to any 'hostile interface') for itself or any other entity," or contract with any third parties to access the system. Dkt. 106-2, at 5. The RCI Agreement contains similar restrictions: "Non-Approved Access" is any access to the Reynolds DMS made without Reynolds' prior written consent. Dkt. 106-3, § 1.8.

E. The aftermath

According to Cottrell, on the heels of the February 2015 agreements, in May 2015, Robert Schaefer, Reynolds' head of data services, told Cottrell that CDK and Reynolds agreed to support one another's data integration programs—3PA and RCI—and block third-party data integrators, like Authenticom. Reynolds was "adamant that all third-party data integrators must be cut off." Dkt. 62, ¶ 52. Schaefer denies making such statements, although the Reynolds/CDK agreements would essentially have this effect.

In August 2015, CDK began aggressively blocking Authenticom. Vendors, many of whom were understanding and willing to work with Authenticom following Reynolds' aggressive blocking in 2013, began to move their business elsewhere. According to Cottrell, Authenticom has been unable to attract new vendor customers because it cannot guarantee that it will be able to provide services without access to Reynolds' and CDK's DMSs.

Cottrell testified that in April 2016, he had a conversation with Dan McCray of CDK. McCray told Cottrell that CDK and Reynolds had agreed to "lock you and the other third parties out." *Id.* ¶ 48. According to Cottrell, McCray stated in no uncertain terms that CDK wanted to destroy Authenticom. Like Schaefer, McCray largely denies that CDK and Reynolds agreed to take concerted action, and he denies the more aggressive statements Cottrell attributes to him. But he does concede that he "confirmed that it was CDK's goal to remove all non-authorized access, including the user ID and password access Authenticom used, from the CDK DMSs in an orderly manner so as to ensure a smooth transition for CDK's dealers, the OEMs, and vendors." Dkt. 95, ¶ 11.

The consequences to Authenticom's business have been severe. Evidence from Authenticom shows a dramatic drop-off in revenue, very limited cash reserves, and breaches of

covenants with its lender on a substantial loan. Authenticom's financial expert, Gordon Klein, testified that Authenticom is on the brink of going under. Without court intervention, Klein estimates that Authenticom will be $1 million in the red over the next 12 months, and Klein would recommend that the bank foreclose on Authenticom's outstanding loan. Defendants' financial expert, Mark Zmijewski, testified that Authenticom has a base of revenue that is not affected by the defendants' blocking, and that there is some residual data integration revenue that is still coming in, including some from non-CDK and Reynolds dealers. He opined that the situation is not as grave as Klein portrays, that the bank would not likely foreclose, and that Authenticom could survive on a reduced scale.

F. Post-agreement competitive effects

Historically, the market for data integration services was competitive, with a number of providers offering services similar to Authenticom's. Now, essentially only Authenticom remains. One other vendor, SIS, is now primarily an application software vendor, but it continues to provide some vestigial data integration services. For the most part, CDK and Reynolds have brought data integration for their dealers in house.

The court received some informative, though not comprehensive, evidence regarding data integration pricing. Although Reynolds' information for pricing RCI integration services is not public, one witness, Alan Andreu, testified that when his software company, Dominion, first began using RCI in 2011, it was paying $247 per month per dealer. Come September 2017, that same data package will cost $893. Andreu also testified that Dominion was paying $457 per dealership for 3PA, CDK's integration service. Dkt. 165, at 39:1-3 ("So compared to Reynolds' 893, it's cheap—it's only $457—until you compare it to that $30 that I could have paid Authenticom."). A second vendor witness, Matthew Rodeghero with AutoLoop, testified

that in 2015, Reynolds charged approximately $700 per month for a dealer using "the full suite of AutoLoop's products." *Id.* at 59:3-5. Now, that price has gone up to $835, plus additional write-back fees. Access to the CDK DMS via 3PA cost approximately $160 in 2014, $694 in 2016, and $735 in July 2017, without "any noticeable product improvements." *Id.* at 62:16-17. CDK concedes that it is now charging vendors more after the 3PA "refresh" initiative.

Defendants attempt to prevent vendors from informing dealers about the price of data integration services. According to Reynolds, its standard RCI vendor contract prohibits the vendor from discussing RCI costs because it would allow for confusing comparisons; each application's RCI interface is individualized, so prices are not comparable. Similarly, CDK prevents vendors from putting a line item on their bills attributable to 3PA charges, to prevent vendors from passing the charge through to the dealer.

G. Security

A few points on security before the court turns to the merits. Schafer testified that the DMSs store customer information, OEM proprietary information, financial information, and other sensitive information. Schaefer testified that Authenticom scrapes data from the Reynolds DMS that it does not need. Reynolds has spent a great deal of time and money developing its "sandbox" system, including customized interface packages, real time access to data, and a journaling feature to track activity and guard against automated errors that may infect the system. In this sense, RCI provides a one-to-one relationship with applications to ensure that they receive only the data they need to serve the dealers.

One witness, Andreu, described Dynamic Reporting—Reynolds' means of allowing dealers to manually extract their data from the DMS—as "comically" and "horribly insecure." *Id.* at 43:7, 13-14. With dealer employees at the helm, it is possible that vendors will receive

pulled data in an unsecured email, unencrypted, despite instructions to upload the data over a secure file transfer protocol (SFTP).

ANALYSIS

To obtain a preliminary injunction, Authenticom must demonstrate that: (1) it has a better-than-negligible chance of success on the merits; and (2) it has no adequate remedy at law and that it would suffer irreparable harm without preliminary relief. *Promatek Indus., Ltd. v. Equitrac Corp.*, 300 F.3d 808, 811 (7th Cir. 2002). Once it satisfies these two preliminary elements, Authenticom must show that the harm it would suffer without the injunction would outweigh the harm that defendants would suffer if the injunction issued. *Id*. Authenticom must also show that the public interest would not be negatively affected by the injunction. *Id*. The stronger Authenticom's case on the merits, the less the balance of harms needs to tip in favor of Authenticom to support the injunction. *Id*.

A. Likelihood of success on the merits

Authenticom brings a number of claims against defendants. For our purposes here, the court will focus on Authenticom's claim that defendants engaged in a horizontal conspiracy, in violation of § 1 of the Sherman Act.

"Every contract, combination . . . , or conspiracy, in restraint of trade or commerce among the several States . . . is declared to be illegal." 15 U.S.C. § 1. Horizontal agreements between competitors are per se illegal. *Toys "'R" Us, Inc. v. FTC*, 221 F.3d 928, 936 (7th Cir. 2000). A plaintiff may prove the existence of a horizontal agreement by either direct or circumstantial evidence. *Id.* at 934. "When circumstantial evidence is used, there must be some evidence that 'tends to exclude the possibility' that the alleged conspirators acted

independently." *Id.* (quoting *Monsanto Co. v. Spray-Rite Serv. Corp.*, 465 U.S. 752, 764 (1984)). "[T]o prove an antitrust conspiracy, 'a plaintiff must show the existence of additional circumstances, often referred to as "plus" factors, which, when viewed in conjunction with the parallel acts, can serve to allow a fact-finder to infer a conspiracy.'" *United States v. Apple, Inc.*, 791 F.3d 290, 315 (2d Cir. 2015) (quoting *Apex Oil Co. v. DiMauro*, 822 F.2d 246, 253 (2d Cir. 1987)), *cert. denied*, 136 S. Ct. 1376 (2016). Market division agreements—agreements to "stay out of each other's territories"—are "per se illegal, just like price-fixing agreements." *Blue Cross & Blue Shield United of Wis. v. Marshfield Clinic*, 152 F.3d 588, 591 (7th Cir. 1998). Group boycotts are per se illegal, too, i.e., "joint efforts by a firm or firms to disadvantage competitors by either directly denying or persuading or coercing suppliers or customers to deny relationships the competitors need in the competitive struggle." *Toys "'R" Us*, 221 F.3d at 936 (quoting *Nw. Wholesale Stationers, Inc. v. Pac. Stationery & Printing Co.*, 472 U.S. 284, 294 (1985)).

Here, Authenticom has adduced evidence that could establish the existence of a per se illegal horizontal conspiracy. Steve Cottrell, Authenticom's founder, owner, and CEO, testified that defendants' representatives—Schaefer and McCray—told him that they had agreed to drive Authenticom from the market. Schaefer and McCray deny making these statements. But their denials were conclusory, whereas Cottrell's testimony was detailed and thus more persuasive. At this point, I will credit Cottrell's testimony.

The February 2015 agreements between CDK and Reynolds also suggest a horizontal conspiracy. Although the agreements do not explicitly state that defendants will work together to eliminate third-party data integrators, the agreements have that effect. The parties agree that they will not attempt to access, or help others access, the *other*'s DMS without permission

(although Reynolds gives CDK a long wind-down period to transition out of the Reynolds integration business). Both parties agree to cooperate in facilitating their dealers' access to each other's software applications. And their agreements with third-party vendors—like the 3PA Agreement and the RCI Agreement—are exclusive, in the sense that defendants agreed that in their capacity as app providers, their sole access to one another's DMSs would be through the in-house interfaces. In other words, by signing up for 3PA or RCI, defendants agreed not to use third-party integrators to access the CDK DMS or the Reynolds DMS, respectively. After the agreements, there is little room in the market for third-party integrators.

Both sides adduced economic experts to explain the parties' conduct here. Authenticom's expert, Hal Singer, testified that when CDK agreed that DMI would wind down its hostile integration practices (with respect to Reynolds, at least), it gave up a competitive advantage: its "toe hold" in the Reynolds market and the opportunity to move Reynolds dealers over to CDK. Before February 2015, CDK was stealing business from Reynolds. After the agreements, it is not clear how CDK benefits. As Singer put it, CDK closed for one of two reasons: either cybersecurity issues really did motivate its move to a closed system, or Reynolds did. Singer suggests that the more reasonable implication is that CDK made an agreement with Reynolds so that it could extract higher prices for data integration services, which would more than offset the loss of dealers who were unhappy with CDK's move to a closed system. Defendants' expert, Sumanth Addanki, testified that the prime interest of both CDK and Reynolds is the DMS market, not the data integration market. And by closing its system, CDK risked losing DMS customers, so the only rational explanation is that CDK closed it system because it saw value in increasing security. It could not have been to increase data integration costs; the value is too small to be worth the trouble.

Neither economic expert had enough data to offer a fully compelling economic explanation for the February 2015 agreements. But Singer's analysis is more supported by the other evidence at the hearing. If a typical dealer uses 10 to 15 applications, and data integration costs are approximately $800 per application, data integration revenue per dealer is nearly the equal of the base cost of the DMS itself. Contrary to Addanki's suggestion, data integration is no sideline. Internal CDK documents also confirm that CDK's decision to refresh its 3PA program was motivated, at least in part, by a desire to realize more revenue from third-party access. And testimony from software vendors suggests that data integration prices have risen considerably, particularly in comparison to prices charged by third-party integrators.

The February 2015 agreements do not explicitly state that defendants agree to work together to freeze out third-party data integrators. But Authenticom has adduced evidence sufficient to suggest more than merely parallel conduct by independent firms.

The court will touch only briefly on Authenticom's remaining Sherman Act claims. As discussed, Authenticom has adduced evidence that suggests that defendants' contracts with vendors are exclusive dealing agreements. "Exclusive dealing involves an agreement between a vendor and a buyer that prevents the buyer from purchasing a given good from any other vendor." *Allied Orthopedic Appliances Inc. v. Tyco Health Care Grp. LP*, 592 F.3d 991, 996 (9th Cir. 2010). Reynolds' standard vendor contract provides that the vendor and its agents are not authorized to directly or indirectly access the Reynolds DMS; they have to use RCI. PHX-53, § 1.9. A similar provision appears in the standard 3PA agreement. DHX-32, at 3 ("Vendor agrees that it will . . . access data on, and provide data to, CDK Systems exclusively through the Managed Interface System[.]").

Unlike horizontal agreements, which are per se illegal, vertical agreements are unlawful "only if an assessment of market effects, known as a rule-of-reason analysis, reveals that they unreasonably restrain trade." *Apple*, 791 F.3d at 313-14. Under the rule of reason, an exclusive dealing arrangement violates § 1 if it forecloses competition in a substantial share of the line of commerce at issue. *Allied Orthopedic*, 592 F.3d at 996. "[A] plaintiff must prove two things to show that an exclusive-dealing agreement is unreasonable. First, he must prove that it is likely to keep at least one significant competitor of the defendant from doing business in a relevant market. If there is no exclusion of a significant competitor, the agreement cannot possibly harm competition. Second, he must prove that the probable (not certain) effect of the exclusion will be to raise prices above (and therefore reduce output below) the competitive level, or otherwise injure competition; he must show in other words that the anticompetitive effects (if any) of the exclusion outweigh any benefits to competition from it." *Roland Mach. Co. v. Dresser Indus., Inc.*, 749 F.2d 380, 394 (7th Cir. 1984).

Here, Authenticom has adduced evidence that defendants have effectively cut it out of the data integration market. And, as discussed above, the court received evidence suggesting that defendants are charging significantly more for data integration through RCI and 3PA than Authenticom charges for data integration. The question here would be whether defendants' higher prices are justified. Defendants explain that the costs are justified because they undertake the burden of maintaining the DMS and preserving its security. I am not persuaded for two primary reasons. First, defendants did not present evidence of the cost of data integration. They presented evidence that they had invested vast sums in their respective DMSs, which is a point taken. But the dealers already pay a lot for the DMS, and defendants did not put in any evidence to quantify the additional expense of providing data integration

services. Second, defendants did not show that properly managed third-party access, even using dealer credentials and screen scraping, really poses additional security risks. Reynolds allows significant exceptions by "whitelisting" certain third parties that it allows to access its system, most notably DMI, CDK's third-party integrator.

Authenticom has made the requisite likelihood of success showing. The court moves to the next factor.

B. Adequacy of legal remedies and irreparable harm

Authenticom must demonstrate that it has no adequate remedy at law. This is a separate consideration from whether Authenticom would suffer irreparable harm, although the considerations are related, and Authenticom presents virtually the same evidence for both.

Typically, a legal remedy is inadequate for one of four reasons: (1) damages would come too late to be of meaningful value to the plaintiff; (2) plaintiff might not be able to afford the full litigation; (3) the defendant might not be collectible at the end of the litigation; or (4) the monetary damages might be too difficult to calculate. *Id.* at 386. Here, Authenticom has adduced compelling evidence that it is on the brink of collapse, which satisfies both options one and two.

As discussed in the fact section, Gordon Klein, Authenticom's financial expert, opined that defendants' continued blocking of access to dealer data would essentially destroy Authenticom's data integration business. Klein opined that without court intervention, Authenticom could be $1 million in the red over the next 12 months. And he predicted that the bank would foreclose on Authenticom's loan.

I do not find Klein's testimony fully convincing, because he has assumed nearly worst-case assumptions about business loss. But the opinions of defendants' financial expert are also

based on assumptions rather than evidence. I find Klein's predictions closer to the mark. Reynolds' blocking, if completely effective, would cut Authenticom out of 28 percent of the market. This would be difficult, but survivable, as Authenticom has demonstrated by largely surviving Reynolds' 2013 blocking efforts by hanging on to CDK. But with CDK also blocking access, Authenticom will be cut off from nearly three-quarters of the dealers in the United States. Most third-party software vendors would be disinclined to engage a third-party integrator that could access data from only a quarter of the dealers in the United States. Authenticom may have some business lines that could survive defendants' blocking—mostly "data hygiene" services—but these services are generic data processing services that are available from many sources, and thus would not be a secure foundation for Authenticom's business that is based on its successful specialized data integration services to dealers and related software vendors.

Every day that Authenticom is unable to serve its customers, it burns more of its goodwill and solidifies its customers' doubts about its viability. Regardless of whether the evidence conclusively establishes that defendants are able to effectively and completely block Authenticom, Authenticom's customer base is growing increasingly wary of continuing to do business with it.

Authenticom has demonstrated that it does not have an adequate remedy at law and that it stands to incur irreparable harm absent court intervention.

C. Balance of harms

Because Authenticom has made its threshold showings, the court considers the balance of the harms to the parties. Defendants contend that a preliminary injunction would harm them in two ways: by imposing increased security risks and overburdening their DMSs.

Cybersecurity. Reynolds made the more substantial showing on this point, so the court will focus on Reynolds. Defendants' security expert, Eric Rosenbach, testified that every point of access to a system is a point of vulnerability. And Reynolds has consistently resisted third-party access using dealer login credentials. Reynolds contends that RCI is more secure, substantially because it is more tightly controlled. Allowing third parties to use dealer login credentials to forage around in Reynolds' DMS renders both dealer data and the Reynolds system less secure. All this is very plausible. But for several reasons, the court is not convinced that Authenticom's access poses significant risks.

First, the evidence at the hearing showed that Authenticom does not forage around or access data beyond the legitimate needs of its customers, vendors and dealers. The court did not hear any evidence that Authenticom takes proprietary OEM data or that any extra information captured in the screen-scraping process is put to ill use.

Second, the court did not hear any evidence that Authenticom has ever experienced a security breach or facilitated a security breach of either defendant's DMS.

Third, Reynolds' Dynamic Reporting function, which Reynolds contends is an acceptable alternative to Authenticom's automated access, poses its own security risks. One witness described the use of Dynamic Reporting by dealer employees as "comically" insecure, because dealer employees often send downloaded dealer data in plain text in unencrypted emails. Dkt. 165, at 43:7, 13-14.

Fourth, Reynolds contends that it is particularly concerned about Authenticom's "machine access" to its DMS. But Reynolds presented no evidence that Authenticom's automated access was less secure than manual access by dealer employees. Also, Reynolds DMS

agreements prohibit dealers from disclosing passwords to non-employees, but they do not specifically prohibit automated access, if done by the dealers or their employees.

Fifth, part of the difficulty of tracking and dealing with third-party access is attributable to Reynolds' blocking efforts, and dealers' and data integrators' efforts to counter the blocking. If Authenticom were to use login credentials created specifically for Authenticom and disclosed to Reynolds, Reynolds should be able to adequately track Authenticom's access and resolve any potential problems associated with that access. The "cat and mouse" game that Schaefer described would be a thing of the past.

Sixth, and perhaps most important, Reynolds already allows many exceptions to its "no hostile integration" policy. There was ample evidence that Reynolds allowed (and even continues to allow to this day) third parties to use dealer credentials when it suited Reynolds. Although Reynolds characterized these exceptions as short-term transitional needs that are tightly controlled, the bottom line is that Reynolds allows many exceptions. And if those exceptions can be managed during a transitional period, it is hard to see how allowing Authenticom temporary access during the course of this trial would impose a serious risk.

I turn now to defendants' contention that Authenticom's access imposes an unwarranted burden on their DMSs. CDK offered evidence that Authenticom made 18,000 queries to CDK's DMS in one day. DHX-186. No one would dispute that Authenticom's queries tax defendants' systems to some degree. But defendants did not submit evidence that would allow the court to determine what proportion of overall system resources were expended on Authenticom's queries. Nor did defendants submit evidence to show how much more resources Authenticom's queries consumed than would have been consumed if the dealers and vendors had used some other, approved means of accessing data. Defendants have not shown

that the Authenticom's access to defendants' DMSs imposes a substantial burden, let alone one that would outweigh the harm to Authenticom if the injunction does not issue.

The balance of harms tips sharply in Authenticom's favor. It faces a very substantial risk of failure without the injunction, whereas defendants could accommodate Authenticom's access to their DMSs substantially with the resources and processes that they already have in place.

D. The public interest

Finally, the court considers the public interest. The court has concluded that a preliminary injunction allowing Authenticom to access dealer data on defendants' DMSs would not pose a substantial security risk. Accordingly, the court concludes that the public would not be disserved by a preliminary injunction.

Moreover, the court concludes that third-party software vendors and dealers would be served by the continued availability of Authenticom's DealerVault software and its data integrations services. Ultimately, if defendants prevail, Authenticom's business model may not be viable. But the court concludes that the public interest is served by providing Authenticom preliminary relief so that it can survive this litigation and, if it prevails, continue to provide a competitive product that has already won acceptance in the market.

E. Injunction formalities

1. Injunction bond

Defendants contend that Authenticom should have to post a substantial bond, "to insure defendants against the substantial risks they would face as a result [of the preliminary injunction]." Dkt. 105, at 65. Defendants ask for $10 million. Authenticom, unsurprisingly,

contends that no bond is warranted and asks that the court waive the requirement. But if the court is inclined to require a bond, Authenticom advocates for $1 million.

Rule 65(c) provides that the court may issue a preliminary injunction "only if the movant gives security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained." "The purpose of an injunction bond is to protect the restrained party from damages that it would incur in the event that the injunction was wrongfully issued." *Bader v. Wernert*, 178 F. Supp. 3d 703, 745 (N.D. Ind. 2016). "[W]hen setting the amount of security, district courts should err on the high side." *Habitat Educ. Ctr. v. U.S. Forest Serv.*, 607 F.3d 453, 456 (7th Cir. 2010) (quoting *Mead Johnson & Co. v. Abbott Labs.*, 201 F.3d 883, 888 (7th Cir.), *opinion amended on denial of reh'g*, 209 F.3d 1032 (7th Cir. 2000)).

Nevertheless, "a number of cases allow a district court to waive the requirement of an injunction bond. In some of these cases the court is satisfied that there's no danger that the opposing party will incur any damages from the injunction." *Id.* at 458. In other cases, the appropriate bond amount exceeded the movant's ability to pay, and courts balanced "the relative cost to the opponent of a smaller bond against the cost to the applicant of having to do without a preliminary injunction that he may need desperately." *Id.* (collecting cases).

Here, the court will not waive the bond requirement, but it will consider Authenticom's circumstances. Authenticom, on the verge of going out of business, is not in a position to post a $10 million bond. The court did not receive compelling evidence regarding potential harm to defendants, either in terms of cybersecurity or the burden on their DMSs. But the court did receive evidence that a preliminary injunction may require defendants to adjust their systems to accommodate Authenticom's access, and that such efforts may be costly. The court will

order that Authenticom post a $1 million bond, an amount that Authenticom concedes is manageable.

2. Form of the injunction

The court will issue a preliminary injunction that will allow Authenticom to access dealer data from defendants' DMSs—with dealer permission—during the pendency of this litigation. But the court will ask the parties to jointly propose the form of injunction. The core provision of the injunction is that defendants are to cease blocking Authenticom from using dealer login credentials to provide data integration services to dealers who authorize Authenticom to provide this service. But defendants may require that Authenticom use login credentials that allow defendants to identify and track the entity or person who is accessing their systems. Defendants may also limit the data accessed by Authenticom to those fields reasonably necessary to the services that Authenticom provides.

The parties will have one week to submit the proposed form of injunction.

ORDER

IT IS ORDERED that:

1. Plaintiff Authenticom, Inc.'s motion for preliminary injunction, Dkt. 51, is GRANTED.

2. The parties will work together to craft the form of the injunction. The parties are ordered to confer and to submit an agreed proposed form of injunction to the court by July 21, 2017. If the parties cannot agree on all terms of the injunction, they should set out their competing proposals in the document.

3. Defendants CDK Global, LLC, and the Reynolds and Reynolds Company's motion to admit preliminary injunction exhibits, Dkt. 168, is GRANTED.

4. Plaintiff's motion to admit preliminary injunction exhibits, Dkt. 170, is GRANTED in part and DENIED in part, consistent with this order.

Entered July 14, 2017.

BY THE COURT:

/s/

_____

JAMES D. PETERSON
District Judge