

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

---

AUTHENTICOM, INC.

Plaintiff,

Case No. 17-cv-318

vs.

Jury Trial Demanded

CDK GLOBAL, LLC; and THE REYNOLDS  
AND REYNOLDS COMPANY

Redacted Version

Defendants.

---

**COMPLAINT**

---

**TABLE OF CONTENTS**

	<b>Page</b>
INTRODUCTION .....	1
PARTIES .....	1
JURISDICTION AND VENUE .....	9
FACTUAL ALLEGATIONS .....	10
I.    The Relevant Product Markets.....	10
A.    The DMS Market .....	10
1.    CDK and Reynolds Dominate the DMS Market .....	11
2.    CDK and Reynolds Maintain Their Market Dominance by Exercising Overwhelming Leverage over Dealerships.....	12
B.    The Dealer Data Integration Market .....	15
1.    It Is Essential that Application Providers Be Able to Obtain Dealer Data Stored on the DMS .....	16
2.    Dealer Data Integrators Provide Dealer Data to Vendors.....	17
3.    Dealers Own Their Data Stored on the DMS .....	21
4.    Dealers Have the Right to Control Who Has Access to Their Data .....	22
5.    Participants in the Dealer Data Integration Market .....	25
a.    Authenticom.....	26
b.    CDK .....	29
i.    Digital Motorworks and IntegraLink .....	30
ii.   CDK Third Party Access Program.....	32
c.    Reynolds Certified Interface Program .....	34
d.    The Remaining Data Integration Providers Have Been Driven from the Market by CDK and Reynolds .....	36

C.	The Single-Brand Aftermarkets for Dealer Data Integration Services .....	37
II.	CDK and Reynolds Have Illegally Agreed To Eliminate Competition in the Dealer Data Integration Market and the Single-Brand Aftermarkets .....	39
A.	The Facts of the Agreement Are Straightforward.....	39
B.	The Purpose of the Agreement Is to Capture Monopoly Profits .....	41
1.	CDK and Reynolds Are Protecting Their DMS Duopoly .....	41
2.	CDK and Reynolds Are Protecting Their Dealer Data Integration Monopolies.....	42
III.	The Evidence of Defendants’ Agreement to Eliminate Competition in the Dealer Data Integration Market and the Single-Brand Aftermarkets Is Overwhelming.....	45
A.	CDK and Reynolds Entered into a Per Se Illegal Written Agreement Dividing the Dealer Data Integration Market and Single-Brand Aftermarkets .....	45
1.	The Agreement Contains Specific Provisions Dividing the Dealer Data Integration Market .....	46
2.	The Agreement Required Coordination in Transitioning Vendor Clients from CDK to Reynolds.....	46
3.	CDK and Reynolds Implemented the Agreement .....	48
B.	CDK and Reynolds Require Dealers and Vendors to Enter into Exclusive Dealing Arrangements That Are Patently Anticompetitive.....	50
1.	Defendants’ DMS Contracts with Dealers Grant Defendants an Exclusive Right to Access the Dealers’ Data .....	51
a.	The Dealer Exclusive Dealing Terms .....	51
b.	CDK and Reynolds Vigorously Enforce the Dealer Exclusive Dealing Provisions .....	52
2.	Defendants’ Contracts with Vendors Grant Defendants an Exclusive Right to Provide Data to Vendors .....	53
a.	The Vendor Exclusive Dealing Terms.....	54

b.	Defendants’ Vendor Contracts Contain Price Secrecy Provisions That Prohibit Vendors from Informing Dealers About the Data Fees .....	55
c.	CDK and Reynolds Vigorously Enforce the Vendor Exclusive Dealing and Price Secrecy Provisions.....	57
3.	The Dealer and Vendor Exclusive Dealing and Price Secrecy Provisions Are Anticompetitive .....	58
C.	Defendants Are Engaged in a Coordinated Campaign to Block Authenticom’s Access to Dealer Data and Thereby Destroy Its Business .....	59
1.	Defendants Have Admitted That They Have Agreed to Restrict Access and Block Authenticom.....	60
2.	Defendants’ Employees Are Working In Concert to Coordinate the Blocking of Authenticom .....	61
3.	Defendants Tried to Coerce Authenticom to Exit the Dealer Data Integration Market.....	61
4.	Defendants Are Blocking Authenticom’s Ability to Provide Dealer Data Integration Services .....	62
a.	CDK and Reynolds Have Disabled Authenticom’s Usernames En Masse .....	63
b.	Dealers Have Protested to CDK and Reynolds and Demanded That They Stop Blocking Authenticom.....	64
c.	Dealers Have Set Up New Usernames for Authenticom, but Those Have Been Quickly Blocked by CDK and Reynolds Too .....	66
d.	CDK and Reynolds Have Refused To Give Credence to the Dealers’ Objections.....	67
e.	CDK and Reynolds Are Proactively Contacting Dealers Served by Authenticom to Pressure Them to Have Their Vendors Switch to the RCI and 3PA Programs .....	67
f.	CDK and Reynolds Have Spread False Information About Authenticom’s Security as Part of Their Marketing Push .....	68

g.	Authenticom Is Losing Its Customers – and Therefore Its Business – Because of Defendants’ Actions .....	70
IV.	Defendants’ Actions Have Harmed Competition .....	71
A.	Defendants’ Anticompetitive Conduct Has Resulted in Massive Price Increases in the Dealer Data Integration Market .....	72
1.	CDK and Reynolds Have Imposed Massive Price Increases As Compared to What Authenticom Charged .....	72
2.	CDK and Reynolds Have Dramatically Increased the Prices for Their Own Data Integration Services.....	73
3.	The Evidence of CDK’s and Reynolds’ Price Increases Is Overwhelming.....	74
4.	CDK and Reynolds Continue to Charge Dealers Escalating Fees for DMS Services .....	75
B.	Defendants’ Anticompetitive Conduct Has Harmed Competition in Many Other Ways.....	76
V.	Authenticom Has Suffered Antitrust Injury.....	78
VI.	Defendants’ Anticompetitive Conduct Has No Pro-Competitive Justification.....	79
	FIRST CAUSE OF ACTION: HORIZONTAL CONSPIRACY IN VIOLATION OF SECTION 1 OF THE SHERMAN ACT .....	82
	SECOND CAUSE OF ACTION: EXCLUSIVE DEALING PROVISIONS IN VIOLATION OF SECTION 1 OF THE SHERMAN ACT .....	84
	THIRD CAUSE OF ACTION: ILLEGAL TYING IN VIOLATION OF SECTION 1 OF THE SHERMAN ACT .....	86
	FOURTH CAUSE OF ACTION: MONOPOLIZATION OF THE DEALER DATA INTEGRATION AFTERMARKETS IN VIOLATION OF SECTION 2 OF THE SHERMAN ACT .....	87
	FIFTH CAUSE OF ACTION: TORTIOUS INTERFERENCE.....	88
	JURY DEMAND .....	89
	PRAYER FOR RELIEF .....	89

## INTRODUCTION

1. Plaintiff Authenticom, Inc. (“Authenticom”) brings this action to remedy and put a stop to ongoing antitrust violations being committed by Defendants CDK Global, LLC (“CDK”) and The Reynolds and Reynolds Company (“Reynolds”). As alleged herein, and supported by voluminous evidence even prior to any discovery, CDK and Reynolds entered into an express horizontal agreement to exclude competition in the market for dealer data integration services, which are critical to the proper functioning of the retail automotive industry. They also imposed unlawful exclusive dealing provisions to reinforce their unlawful horizontal agreement. Authenticom – Defendants’ last remaining competitor in the dealer data integration market – has been crippled by Defendants’ unlawful conduct and will soon be out of business if that conduct is not promptly enjoined. This case is thus critical not only to Authenticom – whose existence as an ongoing concern hangs in the balance – but also to automobile dealers and the suppliers of essential services to those dealers.

2. Dealers’ data is the lifeline of the automotive industry. In the course of their operations, automobile dealerships generate important data, including vehicle and parts inventory, customer name and contact information, completed and pending sales, vehicle financing and insurance information, and much more. Dealers authorize third-party application providers (commonly referred to in the industry as “vendors”) to access their data so that the vendors can provide the dealers with essential services, such as inventory management, customer relationship management, and electronic vehicle registration and titling. Dealer data integration providers such as Authenticom transform the dealers’ raw data into a usable form appropriate to the particular services each vendor provides to the dealer. Vendors depend on and cannot provide their services without access to a dealer’s data.

3. Dealers enter their data into a database within their Dealer Management System (“DMS”). The DMS is the mission-critical enterprise software that manages nearly every function of a dealer’s business. Defendants CDK and Reynolds are by far the two giants of the DMS market, controlling approximately 75 percent of the United States market by number of dealers, and approximately 90 percent when measured by vehicles sold. CDK and Reynolds have enormous leverage over dealers. Not only is it deeply disruptive and expensive for a dealer to switch DMS providers (switching takes up to a year of preparation and training), but CDK and Reynolds use their market power to compel dealers to submit to long-term contracts of between five and seven years in length. As a result, CDK and Reynolds have maintained their duopoly for over three decades. No competitor has been able to touch them – even Microsoft has failed.

4. CDK and Reynolds also provide dealer data integration services – separate and apart from their DMS services – in direct competition with Authenticom.

5. For over a decade, all DMS providers – including CDK and Reynolds – recognized that dealers have the right to grant data access to the integrator of their choice. Everyone agreed – and still agree to this day – that dealers own their data. Reynolds has publicly declared: “The data belongs to the dealers. We all agree on that.” CDK likewise states that it “has always understood that dealerships own their data and enjoy having choices on how best to share and utilize that data with others.” When dealers and vendors had a choice of which integrator to use, the integration market flourished. Over a dozen integrators provided secure, reliable, and cost-effective access to dealer data. With that access, vendors innovated and created numerous new software applications to help dealerships sell and service cars.

6. In 2007, after Reynolds was privately acquired by Bob Brockman, Reynolds changed its position. Reynolds started to block data integrators – including Authenticom and

CDK – from accessing dealer data on the Reynolds DMS by disabling the integrator’s dealer-created login credentials. CDK, like the rest of the automobile industry, criticized Reynolds’ reversal. Steve Anenen, CDK’s CEO, publicly reaffirmed that dealers using the CDK DMS had the right to grant data integrators access to the dealers’ own data. “We’re not going to prohibit that or get in the way of that,” he told an industry publication. “I think we’ve stated pretty emphatically, we really believe the dealer owns the data. I don’t know how you can ever make the opinion that the data is yours to govern and to preclude others from having access to it, when in fact it’s really the data belonging to the dealer. As long as they grant permission, how would you ever go against that wish? I don’t understand that.”

7. Over the next eight years, CDK continued to take that position. In fact, CDK’s own data integration business extracted data for Reynolds dealers even though Reynolds tried to block CDK from doing so. Mr. Brockman of Reynolds was asked about the fact that CDK “will not prohibit dealers from providing their vendors with a user ID and password to extract data.” Mr. Brockman responded: “I don’t understand [CDK’s] position. Other than to be obstinate, than to be opposite, I can’t imagine from a business standpoint that that’s truly their position. And frankly it would be my opinion that after awhile they probably change that position.” In February 2015 – when CDK made an about face and entered into an illegal agreement with Reynolds to restrict access to dealer data – Mr. Brockman got his wish.

8. Specifically, in February 2015, CDK and Reynolds entered into an agreement to eliminate competition in the dealer data integration market. First, they agreed not to compete with each other. Effective February 18, 2015, CDK and Reynolds entered into a formal written contract whereby Defendants agreed that CDK would stop providing integration services for dealers using the Reynolds DMS, ceding that ground exclusively to Reynolds. Moreover, the



written agreement provided for coordination between the Defendants to transition vendors from CDK to Reynolds. On March 2, 2015, CDK sent a letter to its vendor clients – i.e., the ones for whom CDK had pulled data from the Reynolds DMS – announcing that the vendors “will be provided with a roadmap to transition” to the Reynolds integration product, which is what happened over the next months.

9. Having agreed not to compete with each other in the integration market, CDK and Reynolds next took steps to eliminate their remaining competitors. CDK and Reynolds took numerous steps to obstruct dealer data integration providers such as Authenticom from obtaining access to dealers’ data, including, for example, by disabling the login credentials to the DMS system created by dealers to provide authorized access to independent integrators. Defendants also bought several integrators off, sued others, and drove the rest from the market. Defendants have succeeded in eliminating all competition in the data integration market except Authenticom.

10. Defendants have now turned their sights on driving out Authenticom, the last competitor remaining in the market. Senior CDK and Reynolds executives have admitted to entering into an agreement to destroy Authenticom. On April 3, 2016, at an industry convention, Dan McCray (CDK’s Vice President of Product Management) approached Steve Cottrell (Authenticom’s owner and CEO) and said that they should “take a walk.” Mr. McCray led Mr. Cottrell off the convention floor and down a service ramp to a secluded area. Mr. McCray then confirmed the existence of the illegal agreement, stating that CDK and Reynolds had agreed to “lock you and the other third parties out.” In reference to a prior offer by CDK to acquire Authenticom’s business for \$15 million, Mr. McCray confirmed the illegal agreement again, stating that the number was so low because Authenticom’s “book of Reynolds business is worthless to us because of the agreement between CDK and Reynolds.” Mr. McCray then said,

“For god’s sake, you have built a great little business, get something for it before it is destroyed otherwise *I will f\*\*\*ing destroy it.*” Top Reynolds executives have delivered the same message.

11. In furtherance of their agreement to eliminate competition in the data integration market, both CDK and Reynolds have also imposed a series of exclusive dealing provisions designed to foreclose competition by Authenticom. CDK and Reynolds have imposed terms in their DMS contracts with dealers providing that dealers cannot provide access to their data to anyone else, including Authenticom. Likewise, CDK and Reynolds have imposed terms in their vendor contracts that vendors that use CDK or Reynolds data integration services cannot obtain such services from any other provider, including Authenticom. These exclusive dealing provisions mean that any vendor that must do business with CDK or Reynolds cannot also contract with Authenticom to provide data integration services. Compounding this market foreclosure, these exclusive terms last for up to seven years in the case of the dealer contracts, and purportedly *forever* in the case of CDK’s vendor contract. That is, even if the vendor were no longer to use CDK for data integration services, it would still be barred – forever – from obtaining data from any CDK dealer from any other source.

12. On several occasions Defendants sought to persuade Authenticom to abandon competition in the dealer data integration market. But having failed to convince Authenticom to exit the data integration market on its own, CDK and Reynolds have waged an all-out assault on Authenticom by intensifying their blocking activities. Dealers have demanded that CDK and Reynolds stop blocking Authenticom, but to no avail. The plight of a Nebraska Ford dealer is typical. In December 2016, after CDK disabled Authenticom’s login credentials, the dealer protested to CDK: “You do not have our authorization to disable user accounts. It is my data and I decide who has access to it.” CDK responded that it in fact had the right to control access.

Incensed, the dealer responded: “We own the data, CDK doesn’t.” But there was nothing the dealer could do.

13. Defendants’ unlawful conduct has decimated Authenticom’s business. Authenticom once provided integration services for more than 15,000 dealers (out of approximately 17,000 franchised dealers nationwide) and hundreds of vendors. In July 2, 2015, Authenticom had the honor of being singled out by President Barack Obama in a speech in La Crosse, Wisconsin. “In 2002, [Steve Cottrell] started a small business out of his house to help manage data for car companies and dealerships,” the President recounted. He noted that Authenticom’s business was booming and that its “business model was right.” “So this business that began in Steve’s son’s old bedroom,” the President explained, “is now one of America’s fastest growing private companies based in a restored historic building right in downtown La Crosse.” Now, almost two years later, as a result of Defendants’ actions, Authenticom’s business is cash flow insolvent and on the verge of collapse.

14. Defendants’ conduct has harmed not only Authenticom but the market as a whole. Despite the fact that dealers and vendors prefer Authenticom’s better-priced and higher-quality integration services, vendors have had no choice but to leave Authenticom for Defendants’ integration products. “It is with reluctance,” one large vendor wrote to Authenticom, “that I write this email to confirm that we will be transitioning our CDK dealership clients from [Authenticom] to CDK.” The vendor explained that “[t]his move was solely the result of CDK’s aggressive and recurring disablement of our data access credentials . . . . Being forced to do business with CDK is distressing.” Vendors could not sustain the business disruptions caused by Defendants’ blocking, and Authenticom hemorrhaged customers.

15. The anticompetitive harm associated with Defendants' conduct is evidenced by the resulting increase in prices for dealer data integration services. Authenticom charges vendors approximately \$50 per month per dealership connection. Other independent data integrators charged similar rates when they were still in business, as did CDK before it entered into its agreement with Reynolds. Since the unlawful 2015 agreement, CDK and Reynolds have charged vendors on average \$300 per month for the same services, and other vendors as much as \$800 per month.

16. Defendants' only justification for their elimination of competition in the integration market is "data security." But that justification is pretextual. Authenticom has never had a data breach; its security protections and protocols meet or exceed the highest federal standards; if there was ever a security incident (and there never has been one), Authenticom has agreed to indemnify dealers, backing up that promise with a \$20 million dollar cyber liability insurance policy. At bottom, it is the dealer's choice to evaluate the security protections of data integrators, and select the one that meets their standards. "This is just a means of revenue generation for CDK," one Florida dealer wrote. "Let me, the client, worry about my data security by using a vendor such as [Authenticom]. It should be my choice on how I want to secure my data, not CDK's." The choice of which data integrator to use belongs to the dealer. As CDK's CEO once stated, as "long as [dealers] grant permission, how would you ever go against that wish?"

17. Authenticom brings this action to restore competition in the market and choice to dealers and vendors. As described in detail herein, Defendants' horizontal conspiracy to eliminate competition is a per se violation of Section 1 of the Sherman Act, *see infra* Count I; their exclusive dealing arrangements with vendors and dealers are patently anticompetitive and

unlawful under Section 1 of the Sherman Act, *see infra* Count II; the illegal tying of their integration service to their DMS service is unlawful under Section 1 of the Sherman Act, *see infra* Count III; their monopolization of their respective Dealer Data Integration aftermarkets is unlawful under Section 2 of the Sherman Act, *see infra* Count IV; and their tortious interference with Authenticom's contracts with dealers and vendors violates Wisconsin state law, *see infra* Count V.

18. Authenticom seeks to recover the damages it has suffered as a result of Defendants' violations of federal antitrust laws and Wisconsin tort law. In addition, Authenticom also seeks an injunction (1) enjoining Defendants from blocking independent data integrators from serving dealers and vendors; (2) enjoining the enforcement of Defendants' exclusive dealing provisions with dealers and vendors; and (3) releasing vendors from the multi-year terms in their contracts with Defendants so that vendors (and dealers) can select a data integrator of their choice.

### **PARTIES**

19. Formed in 2002, Plaintiff Authenticom is a privately-held Wisconsin corporation with its corporate headquarters and principal place of business at 400 Main Street, La Crosse, Wisconsin 54601.

20. Defendant CDK is a publicly traded Delaware corporation with its corporate headquarters and principal place of business at 1950 Hassell Road, Hoffman Estates, Illinois 60169. CDK provides Dealer Management System ("DMS") software and services to automobile dealerships throughout the United States, including in Wisconsin, and has more than \$2 billion in annual revenues. CDK competes with Authenticom in providing data integration services. In 2014, CDK was spun off from ADP, LLC, and is now an independent, publicly

traded company in which ADP retains no ownership interest. Prior to the spin-off, CDK was referred to as ADP Dealer Services (collectively, referred to herein as “CDK”).

21. Defendant Reynolds is an Ohio corporation with its corporate headquarters and principal place of business at One Reynolds Way, Kettering, Ohio 45430. Like CDK, Reynolds provides DMS software and services to automobile dealerships throughout the United States, including in Wisconsin. Reynolds also competes with Authenticom in providing data integration services. Though formerly a publicly traded company, Reynolds was acquired by Bob Brockman in 2006.

### **JURISDICTION AND VENUE**

22. This action arises under Sections 1 and 2 of the Sherman Act, 15 U.S.C. §§ 1 and 2; Sections 4 and 16 of the Clayton Act, 15 U.S.C. §§ 15 and 26; and Wisconsin state law.

23. This Court has jurisdiction over the federal claims pursuant to 28 U.S.C. §§ 1331 and 1337 and Sections 4 and 16 of the Clayton Act, 15 U.S.C. §§ 15 and 26. This Court has supplemental jurisdiction over the state law claim pursuant to 28 U.S.C. § 1367 because it is so closely related to the federal claims that they form part of the same case or controversy.

24. This Court has personal jurisdiction over Defendants because they have engaged in the unlawful acts described in this Complaint with the foreseeable or intended effect of causing substantial economic harm to Authenticom in Wisconsin. This lawsuit arises from and relates to Defendants’ Wisconsin activities – including their unlawful conspiracy and attempts to block Authenticom’s access to the DMS platforms of hundreds Wisconsin automobile dealerships served by Authenticom. Moreover, Defendants purposefully availed themselves of the privilege of doing business in Wisconsin through the widespread promotion, sale, marketing, and distribution of their products and services in the state.

25. Venue is proper in this District pursuant to Sections 4, 12, and 16 of the Clayton Act, 15 U.S.C. §§ 15, 22, and 26, and 28 U.S.C. § 1391(b), (c), and (d). Defendants are registered to do business, transacted business, were found, and had agents in the District; a substantial part of the events giving rise to Authenticom's claims arose in the District; and a substantial portion of the affected interstate trade and commerce described herein has been carried out in the District.

26. As described throughout the Complaint, Defendants' unlawful conduct has substantially affected interstate commerce by harming competition, increasing prices, reducing quality, and limiting output, to the detriment of Authenticom, dealers, and application providers throughout the nation. *See, e.g., infra* Parts IV, V.

### **FACTUAL ALLEGATIONS**

#### **I. The Relevant Product Markets**

27. The relevant product markets for Authenticom's claims are: (1) the DMS Market in the United States; and (2) the Dealer Data Integration Market in the United States, with the single-brand aftermarkets of (i) the CDK Dealer Data Integration Market and (ii) the Reynolds Dealer Data Integration Market.

##### **A. The DMS Market**

28. Dealer Management System software is enterprise software designed specifically for retail automotive dealerships. The software manages virtually every aspect of a dealer's business. The DMS has been analogized to the central nervous system of a car dealership. Specifically, DMS software handles and integrates the critical business functions of a car dealership, including sales, financing, inventory management (both vehicle and parts), repair and service, accounting, payroll, human resources, marketing, and more. In short, DMS software is the mission-critical software that enables dealerships to run their operations and function as a

business. Industry publications describe the DMS as “the center of a dealer’s entire retail management platform. It’s impossible to operate without it.”

29. Critically, the DMS is also the place where a dealer’s own data is stored, such as its inventory, customer, sales, and service information. In this way, the DMS also operates as a database. The physical storage of the data typically takes place either onsite at the dealership (on servers owned by the dealer or the DMS provider), offsite at private data centers operated by the DMS provider, or with cloud-based data storage companies.

30. A dealer only has one DMS provider at a time. It would be functionally impossible for a dealership to operate with two separate DMS platforms – DMS providers have completely different and incompatible operating software for their respective systems.

31. DMS providers license and sell their software and services to automobile dealers pursuant to written contracts of between five and seven years in length.

32. The DMS market is comprised of those providers that sell and market DMS services to automobile dealerships in the United States. The relevant geographical market is the DMS market is the United States. There is public and industry recognition of the DMS market. There are no reasonable substitutes for the enterprise software and services provided by DMS providers to retail automotive dealerships.

#### **1. CDK and Reynolds Dominate the DMS Market**

33. CDK and Reynolds together dominate the DMS market. Combined, CDK and Reynolds control approximately 75 percent of the DMS market in the United States when measured using dealership rooftops (i.e., franchised stores), with CDK controlling approximately 45 percent of the market and Reynolds controlling 30 percent. When measured using the number of vehicles sold from franchised dealers – which is more relevant for antitrust purposes – CDK’s



and Reynolds' market dominance is even more pronounced with a combined market share exceeding 90 percent.

34. CDK's and Reynolds' domination of the DMS market has been stable for decades. Because of the barriers to entry described below, other DMS providers and new entrants have not been able to break CDK's and Reynolds' stranglehold. *See infra* Part I.A.2.

35. Aside from CDK and Reynolds, the DMS market is diffuse, with an array of providers dividing up the remaining market share. These providers are typically small, occupy a particular niche, and serve the country's smaller car dealerships.

36. Based on the foregoing, industry publications variously describe CDK and Reynolds as "the Big 2," "the Duopoly," "the two 400-pound gorillas," and "the two giants of the DMS market."

37. CDK and Reynolds have enormously lucrative DMS businesses. A single, small dealership will pay up to \$150,000 per year for the DMS software license and services offered by CDK and Reynolds. Mid-size dealership groups (5 to 10 stores) can pay \$1,500,000 or more per year, and large dealerships can easily pay over \$5,000,000 per year. Given the thousands of dealerships that CDK and Reynolds serve, and with profit margins exceeding 40 percent, CDK and Reynolds are tremendously profitable. CDK's market capitalization is \$9.2 billion.

## **2. CDK and Reynolds Maintain Their Market Dominance by Exercising Overwhelming Leverage over Dealerships**

38. CDK and Reynolds have powerful leverage over car dealerships, and they use that leverage to protect their dominant positions and constrain dealers' behavior.

39. First, CDK and Reynolds sell their DMS software and services pursuant to long-term contracts, typically between five and seven years in length, often with automatic extensions

if new services are ordered in the middle of the contract. CDK and Reynolds therefore lock in their dealers with lengthy contracts.

40. Second, it is enormously difficult and disruptive for a dealer to switch DMS providers. One industry executive stated that changing DMS providers “is akin to a heart transplant.” CDK’s CEO recently acknowledged that “switching DMS providers can be very difficult. It [is] quite a process [to] change and takes time, which is part of the reason that many dealers are hesitant to switch.”<sup>1</sup> One large dealer publicly referred to changing DMS providers as “mission impossible.” Both Reynolds and CDK have publicly touted that their market positions are secure because of this very fact. Indeed, the *average* DMS client tenure is over 20 years.

41. Switching DMS providers is so difficult because it disrupts and changes nearly every process that a dealer uses to operate. For a typical dealership to change DMS providers, it takes at least a year of preparation, staff training, and testing before the new system is even put into operation. The financial costs – in terms of training and implementation – are enormous.

42. The experience of Hendrick Automotive Group, the sixth largest dealership group in the country, is illustrative. In May 2016, Hendrick announced that it had decided to switch from Reynolds to CDK, with the goal of completing the transition by mid-2017. The fact that such a large dealership group had decided to switch DMS providers was momentous news in the automotive industry. However, just months later, CDK disclosed that Hendrick had decided against the move. The switchover to CDK had already begun but was halted because of the difficulty, cost, and disruption caused by the attempt. Hendrick remained with Reynolds.

---

<sup>1</sup> Thomson Reuters StreetEvents, *Edited Transcript: CDK – Q1 2017 CDK Global, Inc. Earnings Conference Call*, at 3 (Nov. 2, 2016) (statement by CDK Global CEO Brian MacDonald).

43. Third, the costs of switching DMS platforms are heightened because CDK and Reynolds can paralyze a dealer's business by restricting critical third-party applications from accessing a dealer's data. The DMS houses a dealer's data, and third-party applications must be able to access that data in order to perform important services for the dealership. Although dealers own the data stored on the DMS, CDK and Reynolds have seized control over access to dealer data. CDK and Reynolds can severely disrupt a dealer's business simply by switching off third-party access to essential dealer data, which is precisely what CDK and Reynolds have done here by repeatedly blocking Authenticom and other data integrators. *See infra* Part III.C.

44. Indeed, Reynolds and CDK punish dealerships that try to switch DMS providers. For dealers, that makes switching DMS providers not only a logistical nightmare, but a risky and litigious proposition. There is a large collection of lawsuits brought by CDK and Reynolds against dealers that tried to switch DMS providers. The lawsuits tell the story of how deeply damaging an unsuccessful change in DMS providers can be. One publicized case involved a dealer that had been with Reynolds for over 20 years and tried to change providers. Reynolds and the dealer ended up in court, with Reynolds refusing to release the dealer's data stored on Reynolds' DMS until the dealer capitulated to an out-of-court settlement.

45. Finally, as a practical matter, it is impossible for a meaningful percentage of dealerships to switch DMS platforms in response to abusive conduct by CDK and Reynolds. Only a small percentage of dealers are up for grabs each year – because of the long-term contracts and insurmountable switching costs – which means there is little dealers can do to constrain Defendants' abusive practices by switching DMS providers. Moreover, it is all the more difficult to curb abusive conduct by Reynolds and CDK where, as here, they have coordinated their misconduct. For example, whether a dealer chooses CDK or Reynolds, dealers

will be locked into the same anticompetitive exclusive dealing arrangements, as will the third-party application providers that serve them. *See infra* Part III.B.

46. CDK and Reynolds have exercised such tight control over the DMS Market for so long, and the barriers to entry are so high, that even Microsoft Corp., the global software behemoth, could not compete with Defendants. Microsoft tried to enter the DMS market in 2006 but failed. In trying to take on CDK and Reynolds, a Microsoft executive publicly conceded, “We kind of got ahead of ourselves.”<sup>2</sup> As Mr. Brockman of Reynolds summarized, given the difficulty inherent in breaking into the DMS market, Microsoft and others “will not be an effective competitor in this marketplace.”<sup>3</sup>

#### **B. The Dealer Data Integration Market**

47. Not only is the DMS the enterprise software that enables dealers to operate, but it is also the location in which dealers input and store their own data. The dealer data stored on the DMS includes vehicle and parts inventory, customer name and contact information, completed and pending sales, vehicle service and repair history, manufacturer pricing and rebate details, vehicle financing and insurance information, and much more. Third-party application providers (commonly referred to as “vendors” in the industry) need access to this dealer data in order to perform essential services for the dealer. The Dealer Data Integration Market consists of those companies that provide service to dealers and application providers by pulling dealer data from the DMS, formatting and aggregating it, and then providing it to application providers.

---

<sup>2</sup> David Barkholz, *Dealers Get New Management System Option*, *Automotive News* (Dec. 2, 2012).

<sup>3</sup> Mr. Brockman has made a habit of touting Microsoft’s inability to break into the DMS market. For example, when asked whether Microsoft’s efforts would “affect Reynolds’ business,” Mr. Brockman responded, “there’s not a chance.” *See, e.g., Automotive News* (Feb. 19, 2007) and (Jan. 25, 2009).

**1. It Is Essential that Application Providers Be Able to Obtain Dealer Data Stored on the DMS**

48. Dealers use software “applications” to perform important sales and operational functions. These applications perform services in addition to (or, in some instances, in replacement of) functions provided by the DMS software. Such tasks include vehicle inventory management, customer relationship management, electronic vehicle registration and titling, and scheduling service and repair appointments. A single dealership rooftop typically uses about ten separate application providers (i.e., vendors) – and often more.

49. Vendors depend on and cannot provide their services without access to the data stored on the dealer’s DMS. For example, vendors that provide electronic vehicle registration and titling – a critical service that dealers are legally mandated to provide in some states, including Wisconsin – must be able to retrieve purchaser, vehicle, and financing information about the sale of a car from the dealer’s DMS. Without access to that data, vendors cannot register and title the car with the state.

50. Some applications not only require data that is “pulled” from a dealer’s DMS, but they also need to “push” data back into the database. A prime example of this type of application is customer relationship management software, which helps dealers record and track potential customers. For example, when a car buyer walks into a showroom, the customer’s information and vehicle preferences are first entered into the customer relationship management application, which then handles the relationship to the conclusion of the car sale. To do so, the application requires a dealer’s car inventory, which is “pulled” from the DMS. At the conclusion of the process, the application must then be able to “push” the customer and sales information back into the DMS database.

51. Importantly, CDK and Reynolds also have their own applications for services that are separate from their DMS services. For example, CDK and Reynolds both have customer relationship management applications, and they have a wholly owned joint venture that provides electronic vehicle registration and titling. Therefore, many of CDK's and Reynolds' own applications compete with those offered by third-party application providers.

52. Some of the largest application providers in need of data integration services are the car manufacturers themselves. Companies like Ford, General Motors, and Volkswagen need access to dealer data in order to help manage car and parts inventory, process warranty claims and recall notices, apply rebate and special promotions to car sales, and assist dealers with marketing and lead generation. These manufacturers rely on data integrators to access dealer data, which is essential to the functioning of the entire automobile industry.

53. The only way for application providers to obtain the required dealer data is from the dealer's DMS. The data is not stored anywhere else. Dealers do not store their data on any other system or database. Dealers do not and would not enter the data into a separate, redundant database. As CDK describes it, the data on a dealer's DMS is "irreplaceable."

## **2. Dealer Data Integrators Provide Dealer Data to Vendors**

54. Third-party application providers (i.e., vendors) do not obtain data directly from dealers. Instead, there is a separate market comprised of companies that specialize in extracting dealers' data from DMS databases, aggregating that data and putting it into a standardized format, and then delivering to vendors the specific data required for their applications. (The pulling of data by data integrators is sometimes referred to in the industry as "polling" data.)

Data integrators are able to pull and deliver data in an automated, seamless way without the need for manual intervention by dealers.<sup>4</sup>

55. Before a data integrator can pull data, it must get specific authorization from the dealer. For example, for integrators like Authenticom, dealers must set up separate login credentials for the integrators so that they can access the DMS database to pull the data. Once dealers set up those credentials, the data integrator can automate the pulling of data through user emulation. The user emulation software runs the data reports and captures the data, using the database software in the same way as a user at a dealership would. The only difference is that the integrator automates the process, whereas a user at the dealership would retrieve the data manually. This method for pulling data – sometimes referred to as “data scraping” or “screen scraping” – is standard not only in the dealer data integration market, but also in numerous other industries, such as banking and healthcare, where data must be pulled from databases for use in applications. *See infra* Part VI.

56. Data integrators pull data from the dealer’s DMS database and then convert that data from a raw, unorganized state into a standardized format that is easy for vendors to use. Each DMS provider has its data in different formats, and dealers themselves enter data differently based on their own individual practices. Data integrators interpret, reformat, and translate the disparate data into a standardized format. They additionally correct data-entry errors or anomalies in the data set, such as missing numbers from vehicle identification numbers (“VINs”) or incorrect customer contact information.

---

<sup>4</sup> While data access providers are commonly referred to as “integrators,” there is no actual “integration” between data integrators and the DMS database in the traditional sense of the two fusing or combining. Instead, in this context, “integration” is simply a synonym for data access. An “integrator” serves as a bridge between the dealer data and the vendor.

57. The data integrator then delivers the data to vendors specifically selected by the dealer – i.e., those vendors whose applications the dealer has decided to use. The data provided to the vendor is limited to that which is specifically required by the application. For example, for electronic vehicle registration, the application receives vehicle sale and financing information, but nothing more.

58. At one time, there were numerous participants in the Dealer Data Integration Market. Today, there are only CDK, Reynolds, and Authenticom. As outlined below, Defendants have succeeded in driving every other competitor out of the market. CDK owns two of the largest dealer data integrators in the industry, Digital Motorworks and IntegraLink. Like Authenticom, Digital Motorworks and IntegraLink obtain login credentials from dealers to pull data and then provide that data to vendors.<sup>5</sup> CDK also has a data integration product for direct access to data on the CDK DMS – the “Third Party Access” program. Similarly, Reynolds has an integration product for direct access to data on the Reynolds DMS – the “Reynolds Certified Interface” program. Reynolds does not, however, have a product that pulls data from dealers that use non-Reynolds DMS systems.

59. Dealers authorize but do not pay integrators to pull their data. Instead, vendors pay integrators for their data services. As detailed below, due to Defendants’ market power and anticompetitive conduct, the prices charged by CDK and Reynolds are far higher than Authenticom’s prices – by many multiples – even though there is no difference in the services provided. *See infra* Part IV.A.

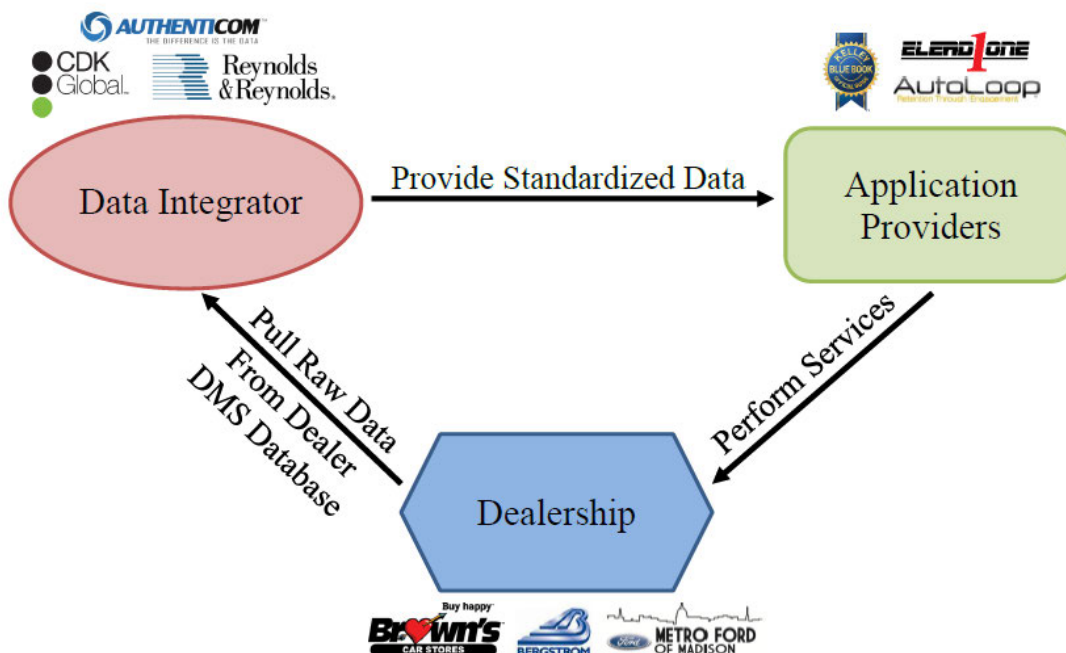
---

<sup>5</sup> As wholly owned subsidiaries of CDK, Digital Motorworks and IntegraLink connect to the CDK DMS via a proprietary CDK VPN, and therefore dealers using the CDK DMS are not required to provide Digital Motorworks and IntegraLink with login credentials to pull data.



60. Vendors enter into contracts with data integrators to pull the data. The length of the contract varies widely depending on the data integrator. While Authenticom’s contracts are for one year, the vendor can cancel services at any time. CDK’s and Reynolds’ vendor contracts are typically three years in length.

61. Below is an illustration depicting how the Dealer Data Integration Market works:



62. Protecting the security of the dealer data is critically important and the responsibility of all entities involved, including dealers, data integrators, vendors, and DMS providers. The most sensitive data pulled by data integrators are the names and contact information (such as home and email addresses) of the dealers’ customers. Importantly, dealer data integrators like Authenticom do *not* have access to the more sensitive categories of data such as social security and credit card numbers. In selecting data integrators, a key criterion dealers and vendors evaluate is the integrator’s security protections and protocols.

63. The Dealer Data Integration Market is comprised of providers of dealer data integration services in the United States. Geographically, the Dealer Data Integration Market is the United States. There is public and industry recognition of the Dealer Data Integration Market. There are no reasonable substitutes for services provided by dealer data integrators, demonstrated most clearly by the fact that Defendants have been able to impose such massive price increases for their data integration services. Moreover, data integration in other markets – such as banking and healthcare – are not reasonable substitutes for data integration in the retail automobile business, where the data owners, vendor customers, and competitors are all different. Nor are DMS services substitutes for data integration, which CDK and Reynolds publicly recognize. Defendants have different businesses that provide data integration – with different pricing – than their DMS services. Moreover, the data integration market has its own supply and demand curves separate and apart from the DMS Market.

### **3. Dealers Own Their Data Stored on the DMS**

64. The data on a dealer’s DMS is not owned by the DMS provider. Rather, the data is owned exclusively by the dealers. CDK and Reynolds have repeatedly admitted this fundamental fact in public statements by senior executives, on their websites, and in their DMS contracts.

65. Tom Schwartz, Reynolds’ chief spokesperson, publicly declared: “The data belongs to the dealers. We all agree on that.”<sup>6</sup> On its website, Reynolds represents to dealers: “Your Data, Your Way. You own your data. Reynolds recognizes you need to share that data outside your dealership.”

---

<sup>6</sup> David Barkholz, *Dealers Decry Reynolds Crackdown*, Automotive News (Nov. 21, 2011).



*News*.<sup>9</sup> “I don’t know how you can ever make the opinion that the data is yours to govern and to preclude others from having access to it, when in fact it’s really the data belonging to the dealer. As long as they grant permission, how would you ever go against that wish?” *Id.*

70. Matt Parsons, CDK’s vice president of sales, similarly stated: “We’re not going to limit the ability of a dealer to give an ID to someone else to, in essence, dial into their system. That is the dealer’s right. We have no right to tell them they can’t do that.”<sup>10</sup> Kevin Henahan, CDK’s senior vice president of marketing, delivered the same message to dealers and the industry: “We don’t tell the dealer, if someone wants access to their data, they have to come to [CDK] to gain access to the data. It’s ultimately the dealer’s data. If he wants to give that data to somebody, for us to try to charge a toll doesn’t seem like the right thing to do. So we’re not going to go down this path.”<sup>11</sup>

71. In addition to these unequivocal statements, CDK benefits from these principles in practice. For more than a decade, CDK’s subsidiaries – Digital Motorworks and IntegraLink – pulled dealer data from *Reynolds*’ DMS using the standard industry method: using login credentials provided by dealers. It was not until CDK and Reynolds entered into their market division agreement in 2015 that CDK changed its policy position and it stopped pulling data from the Reynolds DMS. Even now, CDK still pulls data from dealers using other DMS systems, again using the same industry methods as before. *See infra* Parts I.B.5; VI.

72. Industry organizations have likewise confirmed that dealers have the right to grant data integrators access to dealer data. On February 2, 2007, the National Auto Dealers

---

<sup>9</sup> Ralph Kiesel, *ADP Provides Dealers 3 Options on Data Access*, *Automotive News* (Feb. 19, 2007).

<sup>10</sup> Ralph Kiesel, *NADA Weigh Reynolds Data Security Debate*, *Automotive News* (Feb. 4, 2007).

<sup>11</sup> Ralph Kiesel, *Dealer Security Stirs Insecurity: Vendors Wary of Reynolds Plan for Computer Systems*, *Automotive News* (Dec. 4, 2006).

Association (NADA) and American International Automobile Dealers Association (AIADA), the two largest automobile dealer associations in the United States, issued a “Joint Policy Statement on Data Accessibility.”<sup>12</sup> The purpose of the statement was to “guide the use and protection of data in dealer management systems.” *Id.* The joint statement set forth the following three principles. First, “[d]ealers should control access to the data stored in their dealership management systems.” *Id.* Second, “[d]ealers, not dealership management system vendors or other entities, should have the sole right and the practical means to authorize third parties to access and extract dealer data.” *Id.* And third, “[d]ealers expect all parties involved in storing and using dealer data to . . . refrain from unreasonably impeding dealer-authorized access to dealer data.” *Id.*

73. Individual dealers themselves have made clear that they control who has access to their data. For example, a Lexus dealership in California wrote that “[a]s a dealership owner, I believe that [DMS providers have] no right to deny me access to my own data. By extension, I also retain my rights to distribute my data to chosen vendors who meet my strict criteria for data security.” *See infra* Parts III.B.1; III.C.4; VI.

74. Auto manufacturers, which are some of the largest application providers (i.e., vendors) in the industry, have also defended the right of dealers to control access to their data. For example, after Reynolds changed its policy and began blocking data integrators from pulling dealer data, DaimlerChrysler AG issued a letter to its dealers stating: “A large DMS provider has announced their intent to discontinue the ability of third-party [integrators] to extract data via your DMS . . . . DaimlerChrysler has concern with this new policy, as it may have a significant

---

<sup>12</sup> NADA Press Release, *NADA, AIADA, Issue Joint Policy Statement on Data Accessibility* (Feb. 2, 2007); *see also* Ralph Kisiel, *Automotive News* (Feb. 4, 2007).

impact to your business.”<sup>13</sup> Referring to CDK’s Digital Motorworks and IntegraLink, DaimlerChrysler noted that “[t]hese companies have been polling dealership data on our behalf for over 10 years and have yet to incur a single security breach in the extraction or delivery of our dealership data.” *Id.*

75. Finally, a large coalition of dealers, application providers, data integrators, and DMS providers – including CDK – formed an industry group called Open Secure Access, Inc., which described itself as “a coalition of companies that believe dealers should control access to the data they own and determine how it is used.”<sup>14</sup> CDK was one of the group’s first members, as was Authenticom. The group published a set of basic principles to guide the industry, including that “dealers should control who accesses their data,” “[t]hird parties that have dealer permission to utilize a dealer’s data should be able to access the data through their own efforts or through the services of an independent company,” and “DMS companies should facilitate interaction with all data available to a DMS user by providing technologically advanced means to interact with (read and write) that data, either through a robust set of APIs, system functionality, or direct access to the database.”<sup>15</sup>

## **5. Participants in the Dealer Data Integration Market**

76. At one time, there were over a dozen players in the Dealer Data Integration Market. Today, only three remain – CDK, Reynolds, and Authenticom. CDK and Reynolds drove out the rest from the market, and they have colluded to do the same to Authenticom.

---

<sup>13</sup> Ralph Kisiel, *DaimlerChrysler Fears Data Security Concerns Will Cost Dealers*, Automotive News (Feb. 5, 2007).

<sup>14</sup> Open Secure Access, Inc. Press Release, *Open Secure Access Releases Automotive Retail Data Security Guidelines* (June 28, 2007).

<sup>15</sup> <https://web.archive.org/web/20070304104838/http://www.opensecureaccess.com/>.

**a. Authenticom**

77. Authenticom was founded in 2002 by Steve Cottrell, and he was the only employee for months as he worked to build the business. Authenticom introduced its data integration service in 2004, and it quickly grew to become a market leader. Authenticom pulled dealer data from all of the available DMS platforms – including Reynolds and CDK – using the industry standard (login credentials provided by dealers) and eventually grew to serve 15,000 dealerships and nearly 500 application providers. As Authenticom grew, CDK and Reynolds did not interfere with Authenticom’s pulling of dealer data from their DMS platforms. Instead, they affirmatively supported Authenticom and the burgeoning Dealer Data Integration Market. Vendors benefited from inexpensive, secure access to dealer data and there was an explosion of innovation in third-party applications that transformed how dealers conducted their business. Authenticom and other dealer data integrators played a critical role in this transformation. From a single employee and \$0 in revenue in 2002, Authenticom grew to a business with 120 employees and over \$20 million in revenue in 2014.

78. The current version of Authenticom’s data integration service is called DealerVault, which gives dealers state-of-the-art control over how their data is pulled and shared. It provides a unified user interface where dealers, with the click of a button, are able to add, remove, or change the data sets that Authenticom pulls from the DMS. Authenticom pulls only those data sets that a dealer has specifically authorized. DealerVault also gives dealers the ability to control, with the click of a button, the data that is sent to each of their vendors. The service further provides reports detailing the data Authenticom collected and to whom it was sent, all down to the granularity of a specific data field. Dealers have embraced the product enthusiastically, with over 5,600 dealers signing up.

79. In response to dealer and vendor demand, Authenticom has also developed the capability to “push” dealer data back into the dealer’s DMS. That capability is beneficial to vendors and dealers because it expands the types of services that vendors can provide to dealers. However, Authenticom has only deployed this service to a limited number of vendors and dealers because CDK and Reynolds can too easily obstruct the push of data back into the dealer’s database. Absent Defendants’ anticompetitive conduct, Authenticom would make this functionality more widely available to vendors and dealers.

80. In Authenticom’s agreements with dealers, the Terms and Conditions make clear that (1) Authenticom extracts only that data that the dealer has specifically authorized Authenticom to pull, *see* Authenticom T&C § 3.4; (2) Authenticom sends data only to those vendors selected by the dealership, *see id.* § 5.3; (3) that Authenticom will not use the dealer data for any other purpose, and (4) that dealers maintain ownership over their data, *see id.* In turn, dealers represent and agree that they have the right to grant Authenticom access to pull data from their DMS databases. *Id.* § 7.1.

81. Authenticom’s contracts with vendors dictate that the vendors can use the data only for the services outlined in the contract between the vendor and dealer.

82. Like all data integrators, Authenticom is compensated by the vendors for providing data integration services; with the exceptions noted below, Authenticom generally does not receive payment for its services directly from dealers. Authenticom’s standard pricing to pull data is \$25 for the first data set, and then \$50 for two or more (Authenticom can supply up to seven different data sets). The average price per vendor to pull data is between \$30 and \$40 per dealership rooftop per month. For bi-directional access – i.e., for data “pulled” from the dealer’s DMS database as well as “pushed” back in – Authenticom has charged at most \$75 per



month for that bundled service, and that price included additional services such as data hygiene. Authenticom has a setup fee of \$2,500 for its services, but that works as a down payment credited against the vendor's first invoices.

83. Tellingly, while Authenticom generally does not charge dealers for data integration services, there are a handful of large dealership groups that choose to pay for DealerVault because of their preference for Authenticom's data integration product – even though the dealers' vendors already are paying CDK and Reynolds for data integration services.

84. Authenticom's security practices are state of the art. Authenticom has never had a data breach and its firewall has never been compromised. Authenticom transfers all data using secured and encrypted protocols that meet or exceed federal standards for federally insured banking transactions. Authenticom partners with Microsoft Azure cloud services – and has achieved Microsoft's top-level gold security certification three years in a row – to provide dealers with a secure place to syndicate and distribute their data.

85. Authenticom's information security system exceeds applicable consumer privacy and protection restrictions, including the Gramm-Leach-Bliley Act of 1999 and the Federal Trade Commission's Implementing Rules. Indeed, Authenticom's contracts with dealers guarantee compliance with those regulatory requirements. Finally, Authenticom agrees to indemnify dealers in the event there is any data security event and backs up that promise with a \$20 million cyber liability insurance policy.

86. Authenticom is very proud of the business it has built and the employment opportunities it provides to the people in and around La Crosse, Wisconsin. Authenticom and Steve Cottrell had the honor of being singled out by President Barack Obama in a speech in La Crosse on July 2, 2015, where the President praised the company for its admirable business and

the positive impact it has had on the community. The President noted that during the recession of 2007-09, “Steve invested in new people, new technology; decided to double down, was absolutely confident his business model was right.” When “the auto industry came roaring back, things began booming,” the President continued. He explained: “Steve’s revenue is up 1000 percent. His company, Authenticom, has gone from 18 employees to more than 120. So this business that began in Steve’s son’s old bedroom is now one of America’s fastest growing private companies based in a restored historic building right in downtown La Crosse.” The President commented how fortunate Authenticom was “to be part of a community like La Crosse: to be part of an industry that got back to basics, determined to do things better and smarter. He pays his employees fair wages. He guarantees paid sick days. He helps pay for the tuition of those folks when they decide to go back to school.”<sup>16</sup>

87. President Obama gave his speech on July 2, 2015, just after CDK and Reynolds had secretly entered into an illegal agreement to divide the data access market and destroy independent data integrators like Authenticom. As detailed below, less than nine months later, a senior CDK executive told Mr. Cottrell that CDK and Reynolds had agreed to “lock you and the other third parties out” and that Mr. Cottrell should “get something for [his business] before it is destroyed otherwise I will f\*\*\*ing destroy it.” This lawsuit is about CDK and Reynolds making good on that threat.

**b. CDK**

88. CDK owns two of the largest dealer data integrators in the industry, Digital Motorworks and IntegraLink. It also has an integration product for direct access to dealer data on the CDK DMS – the 3PA program.

---

<sup>16</sup> For the President’s full remarks on Authenticom, *see* [www.youtube.com/watch?v=Bfzu9kd5HU8](http://www.youtube.com/watch?v=Bfzu9kd5HU8).

**i. Digital Motorworks and IntegraLink**

89. Like Authenticom, Digital Motorworks and IntegraLink obtain authorization from dealers to pull data (using login credentials and data scraping) and provide that data to vendors. At the time CDK acquired Digital Motorworks in 2002, CDK stated: “As a result of its acquisition of Digital Motorworks, [CDK] now has the ability to extract, transform and standardize data from varied sources to client specifications.” Digital Motorworks claims to work with over 100 vendors and pull data from thousands of dealerships.

90. CDK acquired IntegraLink in 2010. IntegraLink – like Digital Motorworks and Authenticom – “specialize[s] in the collection of data from automotive retailers’ dealership management systems” using the same standard process. IntegraLink was founded in 1998 by Kevin Distelhorst to “fill the need for a professional data collection firm focused entirely on the needs of the automotive retailing industry.”<sup>17</sup> Prior to founding IntegraLink, Mr. Distelhorst was Reynolds’ director of online services. Today, Mr. Distelhorst is a vice president at CDK.

91. For over a decade – before CDK and Reynolds entered into their market division agreement – Digital Motorworks and IntegraLink pulled data from Reynolds dealers using login credentials, instructing dealers to provide them with a “dedicated account” and password. *See, e.g.,* [https://www.integralink.com/hyundai/acct\\_check.html](https://www.integralink.com/hyundai/acct_check.html) (“Reynolds [DMS] dealers should provide user ID, password, and store number with access to program 2213 & 6910 (report generator).”).

92. During much of that time period, Reynolds did not block CDK’s access to dealer data – just as it did not block Authenticom and other dealer data integrators. Reynolds did not start blocking CDK and others in earnest until 2011. Thereafter, Reynolds blocked and disabled

---

<sup>17</sup> IntegraLink, *About Us: Kevin Distelhorst*, [www.integralink.com/about\\_management\\_kd.html](http://www.integralink.com/about_management_kd.html).

CDK's usernames, disrupting Digital Motorworks' and IntegraLink's pulling of data. As described by CDK to dealers at the time, "Reynolds has instituted policies designed to prevent automated processes such as those used by IntegraLink, [Digital Motorworks,] and other third-party data-collection services from collecting data for programs you have enrolled in."<sup>18</sup> "In short," CDK explained, "when Reynolds blocks our access to your data on your dealership management system, we cannot perform the tasks you have asked us to perform." *Id.*

93. To circumvent Reynolds' blocking, CDK rolled out a new solution called "SMART-R." As described by CDK, the application "automates the process of running [Reynolds DMS data] reports (7601/7602), captures and encrypts the output, and then securely transfers the data to IntegraLink" or Digital Motorworks. *Id.*

94. In short, with the help of its workaround, CDK continued to pull data of dealers using the Reynolds DMS. That state of affairs abruptly changed in February 2015, when CDK and Reynolds entered into an agreement to divide the data integration market. Pursuant to this agreement, CDK agreed that it would no longer compete with Reynolds in providing integration services for dealers using the Reynolds DMS. *See infra* Part III.A. After the agreement, Digital Motorworks and IntegraLink discontinued their data pulling business for dealers using the Reynolds DMS, ceding that ground exclusively to Reynolds.

95. Significantly, CDK – through Digital Motorworks and IntegraLink – continues to pull data from dealerships using non-Reynolds DMS systems precisely as before. For most DMS systems, dealers provide CDK with login credentials. The other DMS providers provide CDK with an API for direct access to pull dealer data. No matter how it obtains the data, CDK

---

<sup>18</sup> IntegraLink, *Smart-R for Reynolds ERA Dealers*, [https://il.dmotorworks.com/downloads/smartr/SMART-R\\_FAQ.pdf](https://il.dmotorworks.com/downloads/smartr/SMART-R_FAQ.pdf).

charges vendors only \$25 to \$50 per connection – pricing that is similar to Authenticom’s – for data pulled from dealers using non-Reynolds DMS systems.

**ii. CDK Third Party Access Program**

96. CDK provides access to dealer data on the CDK DMS through an official data integration product called the Third Party Access, or 3PA program.

97. Before February 2015 – when CDK and Reynolds entered into their illegal agreement – the 3PA program had three levels. The first level was “basic access” by which a dealer “supplie[d] third-party vendor[s] a user ID and password to access the dealership’s system.”<sup>19</sup> This level of access was a recognition that dealers have a right to grant access to their data to whomever they wish, and CDK imposed no charges for this. The second level was “subscriber access” in which CDK “provide[d] secure, high-speed Internet access” to the DMS, with the “[d]ealer maintain[ing] responsibility for data access.”<sup>20</sup> CDK charged a small amount for the Internet service. The final level was “Third-Party Integration,” which was data access obtained directly from CDK and included “real-time access” and a “bi-directional interface,” allowing for both pulling data from and pushing data into the DMS. *Id.* CDK’s prices for this increased level of data access were higher than the prices charged by Authenticom, averaging approximately \$70 per month per dealership rooftop. Importantly, dealers could choose access levels on a vendor-by-vendor basis, giving dealers flexibility in managing how their vendors obtained data.

98. This changed after CDK and Reynolds entered into their market division agreement in February 2015. CDK scrapped the old version of the 3PA program in exchange for one that matched Reynolds’. CDK now blocks dealers from granting third-party data integrators

---

<sup>19</sup> Ralph Kisiel, *ADP Provides Dealers 3 Options on Data Access*, Automotive News (Feb. 19, 2007).

<sup>20</sup> *Id.*; Automatic Data Processing, Inc., *ADP’s Third Party Access Program*.

(like Authenticom) access to dealer data. The revised 3PA program requires all vendors to obtain data directly from CDK – and at much higher prices. On average, CDK now charges vendors on average between \$250 and \$300 per connection, almost triple the \$70 that it charged before for the exact same services. When compared to the \$25 to \$50 per connection that CDK (through Digital Motorworks and IntegraLink) charges for integration services on non-CDK platforms, the price increase is even more stark. Moreover, for “bi-directional” access – that is, for both “pulling” data from the DMS and “pushing” data back into the database – CDK charges vendors up to \$700 per connection.

99. CDK announced the revamped 3PA program on June 22, 2015, as part of its “SecurityFirst” initiative. This initiative used data security as the excuse for stripping dealers of control over access to their own data and imposing massive price increases on vendors. The industry saw this for what it was. “CDK is rolling out a new cybersecurity initiative,” *Automotive News* reported, “that will raise monthly integration fees for most of the third-party software vendors that dealerships use in addition to CDK software. It is patterned after a program at Reynolds and Reynolds.”<sup>21</sup> Vendors and dealers received little, if anything, in return for the dramatically higher prices. “Vendors briefed on CDK’s new data-security program said nothing will change in the way they get data from CDK-served DMS dealerships under SecurityFirst except for a higher price.”<sup>22</sup> Indeed, vendors “in the CDK program . . . say the costs being charged far exceed the value of any increased data security.” *Id.* One “vendor executive who asked not to be named called the data-access cost a surcharge under the guise of data security.” *Id.*

---

<sup>21</sup> David Barkholz, *CDK Global Sees Earnings Boost from Cost-Cutting, Improved Efficiency*, *Automotive News* (Nov. 3, 2015).

<sup>22</sup> David Barkholz, *Dealers Will Pay Up for Vendors’ Data Access After CDK Switch*, *Automotive News* (July 20, 2015).

100. CDK has also engaged in deceptive advertising with respect to the new higher pricing. As part of the revamped 3PA program, CDK posted a pricing guide on its website that CDK represents is the standardized pricing for all vendors. “Our 3PA pricing philosophy is simple,” CDK states in its program guide, “standardized pricing for all customers.” But that is false. As many vendors can attest, CDK imposes much higher prices than what it advertises. For example, CDK told one vendor providing electronic vehicle registration and titling that the vendor would have to pay 25 percent of its top-line revenues to participate in the 3PA program, which is many times more than the posted “standard” pricing.

101. Today, CDK declares that the 3PA program is the “only approved method for accessing” data on a dealer’s DMS. It labels any other method for accessing data – including through data integrators such as Authenticom – as “unauthorized.” According to CDK, a dealer breaches its contract when it provides so-called “unauthorized” access to data integrators. Moreover, unlike before, CDK now contractually forbids vendors from obtaining data from anyone but CDK. In this way, CDK has perfected its power grab, making the 3PA program the only means by which vendors can obtain the necessary data for dealers using the CDK DMS.<sup>23</sup>

**c. Reynolds Certified Interface Program**

102. Reynolds provides access to dealer data on the Reynolds DMS through the Reynolds Certified Interface, or RCI, program, which is Reynolds’ equivalent to CDK’s 3PA data integration product.<sup>24</sup> Before Mr. Brockman acquired Reynolds, Reynolds operated like all

---

<sup>23</sup> As discussed above, car manufacturers are some of the largest and most important vendors in need of data integration services, for purposes of recalls, rebates, inventory, and many others. While not formally participants of the RCI or 3PA programs, CDK and Reynolds provide data integration services to car manufacturers just as they do to other vendors, and charge similarly high rates.

<sup>24</sup> Reynolds does not have an independent data integration business that pulls data from other DMS platforms. Therefore, unlike CDK with its Digital Motorworks and IntegraLink businesses, Reynolds does not compete in the Dealer Data Integration Market outside of the Reynolds DMS.

others in the industry. Dealers were free to have data integrators pull their data in automated ways by using login credentials and user emulation software. But Mr. Brockman put a stop to that in the name of “security” and transformed the RCI program into the exclusive method for automated access to data on the Reynolds DMS, imposing large price hikes in the process. Prior to 2015, CDK even used Reynolds’ blocking of data access as a marketing tool to convince dealers to switch DMS platforms, and some dealers did switch from Reynolds to CDK on reliance that CDK would not take the same position. But now that CDK blocks independent integrators just like Reynolds, there is no difference between them.

103. The RCI program operates in nearly identical ways to CDK’s 3PA program. Like the 3PA program, the Reynolds RCI program is the only means by which vendors are allowed to obtain automated access to dealer data on the Reynolds DMS. Like CDK, Reynolds blocks third-party access to dealer data, disabling credentials created by dealers for other data integrators. Like CDK, Reynolds contractually restricts both dealers and vendors from using competing integrators. And like CDK, Reynolds charges exorbitant rates for access to the data.

104. Reynolds does not publicize its data integration pricing. According to current and former Reynolds executives, Reynolds has a pricing committee (chaired by the company’s owner, Mr. Brockman) that determines the rates on a vendor-by-vendor basis. Based on information from several sources, the data integration fees under the RCI program are even steeper than CDK’s under the 3PA program. *See infra* Part IV.A.

105. Finally, Reynolds has a tool called “Dynamic Reporting,” which is a non-automated function for dealers to manually generate a data report. Dealers must manually generate the report (or reports), and then send the necessary data to a vendor every time the vendor requires the data for its application. Authenticom has tried to help dealers cut down on



the manual steps for using Dynamic Reporting, but the tool still requires a dealer's daily manual intervention. The tool is useless for applications requiring regular data feeds or bi-directional access to dealer data, and dealers do not have the personnel available to initiate the process multiple times per day. Given these shortcomings, dealers and vendors generally refuse to use the Dynamic Reporting tool for their integration needs except in limited, one-off cases.<sup>25</sup>

**d. The Remaining Data Integration Providers Have Been Driven from the Market by CDK and Reynolds**

106. The Dealer Data Integration Market once had numerous participants. But CDK and Reynolds have systematically destroyed or driven them all out of the market (other than, as yet, Authenticom). To achieve that result, CDK and Reynolds have blocked access and disabled usernames, filed lawsuits, and required data integrators to leave the market as a condition of allowing certain third-party applications to participate in the 3PA and RCI programs (where the company that owned the data integration business also had third-party applications that required access to dealer data). A few examples follow.

107. Superior Integrated Solutions, Inc. ("SIS") was a leading data integration provider, servicing thousands of car dealerships. CDK and Reynolds excluded SIS from the market through blocking and litigation tactics. Reynolds first sued SIS for tortious interference, claiming that by having dealers grant SIS access to their data, the dealers were in breach of their DMS contracts. After years of bruising litigation, SIS settled and left the integration market for dealers using the Reynolds DMS. Then, in August 2016, under the threat of blocking and password-disabling, CDK forced SIS to shut down its integration services for dealers using the

---

<sup>25</sup> And even with these shortcomings, Reynolds has still made it difficult for dealers. At one time, the tool had a bulk export functionality so that dealers could export multiple data reports at once. But when Authenticom helped dealers automate that functionality, Reynolds disabled it, only turning it back on after dealer complaints.

CDK DMS. In short order, SIS went from one of the most successful data integration providers, with a long litany of clients, to a bygone participant in that market.

108. SelectQu, which is owned by Dominion Enterprises, is another dealer data integrator that was forced out of the market. SelectQu's parent company (Dominion) provides a large number of software services in the automobile market and owns several popular applications that provide inventory, reputation management, and customer relationship management services for dealers. In order to obtain approval for participation in the 3PA and RCI programs for these applications, CDK and Reynolds forced Dominion to agree that SelectQu would no longer pull data from their DMSs. As a result, SelectQu exited the market, forced out not only by the usual blocking and disabling of usernames, but also by the leverage Defendants hold over applications needing dealer data from their customers.

109. The list goes on. New Freedom Data Resources – founded in 1991 and a pioneer in the market – was forced to shut down its data integration business in 2014 as a result of Reynolds' blocking actions. The StoneEagle Group recently ended its data integration business in exchange for CDK and Reynolds allowing its data analytics application into the 3PA and RCI programs. ProQuotes, Inc. was cut off from accessing data on CDK DMSs in the fall of 2016, and as a result exited the data integration market. There are still others, all victims of CDK's and Reynolds' strong-arm tactics.

110. In short, CDK and Reynolds have succeeded in eliminating virtually all competition in the data integration market for dealers using the CDK and Reynolds DMS platforms, and have now targeted Authenticom, their only remaining competitor.

### **C. The Single-Brand Aftermarkets for Dealer Data Integration Services**

111. The markets for dealer data integration for dealers using Defendants' DMS systems are cognizable, brand-specific antitrust aftermarkets.

112. The aftermarket for dealer data integration is derivative of the primary DMS Market. If there were no DMS systems in the first place, there would be no demand for integration services for dealer data on those systems.

113. When dealers purchase a DMS system, they are “locked in” to that purchase through high switching and information costs. As explained above, CDK and Reynolds lock their DMS customers into long-term contracts. Even aside from the long duration of the contracts, switching DMS providers is expensive and difficult – which is why the average car dealer stays with a single DMS provider for an average of 20 years.

114. Information costs prevent dealers from accurately factoring in Defendants’ higher data integration fees when they choose their DMS provider. Among other things, CDK and Reynolds are not transparent with dealers about their data integration fees. On the contrary, and as explained *infra* Part III.B.2.c, Defendants impose price secrecy provisions on application providers, which frustrates the flow of information and prevents dealers from engaging in accurate lifecycle pricing. Similarly, dealers had no reason to believe Defendants would switch positions with respect to data access after CDK and Reynolds had already locked them into long-term DMS contracts. For example, given CDK’s unequivocal public statements, dealers could not have known that CDK would make an abrupt change and seize control over access to dealer data.

115. Because of these market imperfections, Defendants can profitably charge – and have charged – supracompetitive prices in the aftermarkets for dealer data integration on their respective systems. That Defendants have been able to impose such large price increases for integration services in their respective aftermarkets demonstrates that there are no reasonable substitutes for services provided by CDK and Reynolds in those aftermarkets. Similarly,

Defendants' integration services on their respective systems are not interchangeable substitutes for one another. Among application providers, there is separate demand for integration services on the two systems. Application providers that want to sell their products to dealerships that use the CDK DMS system functionally must purchase data integration services from CDK. The same is true for Reynolds dealerships. If CDK's and Reynolds' integration products were reasonable substitutes, application providers would choose between them. But instead, application providers buy *both* CDK and Reynolds dealer data integration services – which would make no sense if the services were interchangeable.

116. As a result of Defendants' actions – including their agreement not to compete, their dealer and vendor exclusive dealing provisions, and their blocking of competing independent data integrators (driving nearly all of them out of business) – CDK and Reynolds have monopolized their respective dealer data integration aftermarkets. Specifically, CDK has a nearly 100 percent market share for dealer data integration services for dealers using the CDK DMS, and Reynolds has the same for dealers using the Reynolds DMS.

## **II. CDK and Reynolds Have Illegally Agreed To Eliminate Competition in the Dealer Data Integration Market and the Single-Brand Aftermarkets**

### **A. The Facts of the Agreement Are Straightforward**

117. No later than February 2015, CDK and Reynolds entered into an agreement to eliminate competition in the Dealer Data Integration Market and the single-brand aftermarkets. The agreement has given CDK exclusive control over data for dealers using the CDK DMS, and Reynolds the same for dealers using the Reynolds DMS. By seizing control over access to dealer data, CDK and Reynolds have been able to impose massive price increases for their data integration services and obtain monopoly profits.

118. As described in more detail below, Authenticom has already uncovered substantial evidence demonstrating Defendants' agreement to eliminate competition in the Dealer Data Integration Market and the single-brand aftermarkets, including the following: (1) In February 2015, CDK and Reynolds entered into a written market division agreement in which they agreed not to compete in the markets, *see infra* Part III.A; (2) Senior executives at both CDK and Reynolds have admitted to Authenticom's President, Steven Cottrell, that Defendants were engaged in a coordinated effort to block independent data integrators like Authenticom and drive them from the market, *see infra* Part III.C.1; (3) CDK and Reynolds have employees working together to effectuate the blocking of independent data integrators, *see infra* Part III.C.2; (4) CDK and Reynolds have jointly included patently anticompetitive exclusive dealing provisions in their agreements with dealers and vendors, securing for themselves the exclusive right to pull dealer data and then provide it to vendors, *see infra* Part III.B.

119. CDK's and Reynolds' decision to divide the market, block other data integrators, and seize control over access to dealer data was the function of an agreement between them, not unilateral decision-making. CDK and Reynolds – horizontal competitors in the DMS Market and, before their market division agreement, one-time competitors in the Dealer Data Integration Market – coordinated their actions and have actively worked together to achieve their aim. Their conspiracy is a per se violation of the Sherman Act.

120. CDK's and Reynolds' conspiracy was formed and implemented by top-level executives at each company. For CDK, the leading actors in the conspiracy include Robert N. Karp, the President of CDK North America and the person with oversight of CDK's 3PA program; Howard Gardner, CDK's Vice President and Manager of Data Strategy and the person who took the lead on the market division agreement; Dan McCray, CDK's recently retired Vice

President of Product Management and the person who told Mr. Cottrell that CDK and Reynolds had agreed to destroy Authenticom's business; and Kevin Distelhorst, CDK's Chief Customer Officer, the founder of IntegraLink, and a former executive at Reynolds. Upon information and belief, other senior CDK executives were also involved in planning, executing, and implementing Defendants' unlawful agreement.

121. For Reynolds, the leading actors in the conspiracy are Bob Brockman, Reynolds' Owner, Chairman, and CEO, and the person who approved the market division agreement and formulated the policy to eliminate competition through blocking; and Robert Schaefer, Reynolds Director of Data Services and the person in charge of the RCI program. Upon information and belief, other senior Reynolds executives were also involved in planning, executing, and implementing Defendants' unlawful agreement.

**B. The Purpose of the Agreement Is to Capture Monopoly Profits**

122. The purpose of the agreement between CDK and Reynolds is twofold: (1) to protect their duopoly and market power in the DMS Market, and (2) to obtain and maintain respective monopolies over the CDK and Reynolds aftermarkets in the Dealer Data Integration Market.

**1. CDK and Reynolds Are Protecting Their DMS Duopoly**

123. Defendants' DMS businesses are money machines. CDK and Reynolds have market power to ratchet up pricing every year. *See infra* Part IV.4. Despite the ever-increasing costs, CDK and Reynolds have maintained their duopoly in the DMS Market for over three decades, and likely much longer. No competitor has been able to touch them. CDK and Reynolds have enduring competitive advantages given their lengthy DMS contracts, high switching costs, and leverage over dealers. *See supra* Part I.A.2.

124. Application providers, however, pose a threat to the CDK / Reynolds duopoly. There are many applications that increasingly perform functions that were once exclusively provided by DMS software, especially those involving inventory and customer relationship management. Such applications – and many others – increasingly have the potential to supplant portions of the DMS software. But such applications cannot be provided without access to dealer data. For this reason, the ability of dealers to provide application providers with inexpensive access to the dealers’ own data is the number one threat to Defendants’ DMS duopoly. That is a reason why CDK and Reynolds have taken such extreme measures to seize control over access to the data. When dealers are allowed to grant access to their data to whomever they wish, Defendants’ duopoly is threatened. Unwilling to take that risk – which is the risk of losing the enormous DMS profits they extract through market power in the DMS Market – CDK and Reynolds have locked down access to dealer data, seizing for themselves the exclusive right to access and distribute it.

**2. CDK and Reynolds Are Protecting Their Dealer Data Integration Monopolies**

125. CDK’s and Reynolds’ incentive to block dealers from providing their data to third parties is not limited to concern over the threat to their DMS duopoly. With respect to the Dealer Data Integration aftermarkets, the 3PA and RCI programs have been rapidly growing cash cows. By 2019, the RCI and 3PA programs will bring in over \$1 billion in combined revenue. The profit margins for their data integration businesses are staggering, exceeding at least 50 percent. By eliminating all competition – especially where other data integrators provided the same services at much lower rates – CDK and Reynolds have been able to impose massive price increases for data integration services and thereby reap monopoly profits from vendors, above and beyond the profits they can charge dealers in the DMS Market. The purpose of Defendants’

agreement to block and eliminate the ability of other competitors, like Authenticom, to compete in the Dealer Data Integration Market is to protect the flow of these monopoly profits.

126. After CDK rolled out its revamped 3PA program, CDK's CEO (Mr. Anenen) remarked – in a case of severe understatement – that the third-party data security program would provide “a lift” in revenue.<sup>26</sup> Indeed, CDK announced massive projected profit growth almost immediately after implementing “SecurityFirst” and entering into the market division agreement with Reynolds. On July 29, 2015, Mr. Anenen told analysts during a year-end earnings call that, on the strength of cost-cutting and better bundling of software products, CDK expected adjusted earnings to rise “at least 25 percent” in 2016.<sup>27</sup> CDK outperformed Mr. Anenen's own projections, and adjusted earnings rose 28 percent in 2016.

127. The widely read Banks Report – the industry's leading newsletter – commented on Defendants' motives: “It's clear, part of that playbook involves charging third-party vendors significantly more for access to the data. It's one area that can provide an almost immediate bump to the bottom line. And as [CDK's] activist investors reportedly are looking for a quick exit, any increase to the bottom line will make for a better sales price.”<sup>28</sup> Another widely read industry publication said, “We see the direction that the DMS companies are moving for adding access fees through the guise of certification and security measures. The incremental costs being added are exorbitant (200, 300 and up to 500% increases in [data integration] fees) to [vendors], and end up coming back to the dealer in the form of higher monthly service fees for all applications using the dealer's data.”<sup>29</sup>

---

<sup>26</sup> David Barkholz, *CDK Global Sees Earnings Boost from Cost-Cutting, Improved Efficiency*, Automotive News (Nov. 3, 2015).

<sup>27</sup> David Barkholz, *CDK Sees 25 Percent Profit Growth in 2016*, Automotive News (July 29, 2015).

<sup>28</sup> Cliff Banks, *Data Access Battle Goes Nuclear*, The Banks Report (Oct. 12, 2015).

<sup>29</sup> Brad Korner, *Dealers Taking Control of DMS Data*, Driving Sales (July 31, 2015).



128. The fact that CDK and Reynolds – rather than the dealers themselves – profit from charging vendors for access to the dealers’ own data is a prime example of the imbalance of power between the dealers and the DMS providers. Indeed, in nearly every case, the vendors pass the cost of access to dealer data on to the dealers themselves in the form of higher service fees – in effect, dealers have to pay CDK and Reynolds for access to their own data.

129. In an article entitled “The Hidden Data Tax That Dealers Don’t Know They Are Paying,” a leading industry publication explained that “[b]ehind dealership DMS systems, there is a big fight taking place worth hundreds of millions of dollars that few dealers know about, despite its potential to take huge profits from the bottom line.”<sup>30</sup> As the publication reported, the “elephant in the room is how much money third parties must pay to access the DMS data on behalf of a dealership, and how those charges are hidden as they are passed on down to the dealers. It’s as if there is a massive ‘data tax’ being paid by most dealerships that few know they are paying, let alone how much they are paying. Because it’s an unknown, it is currently near impossible to manage, and such a tax has large effects on dealership profits and technology innovation.” *Id.* This article was written in 2013, before CDK and Reynolds entered into their agreement and when there was still somewhat robust competition in the Dealer Data Integration Market. Today, the situation is much worse, with the “data tax” imposed by CDK and Reynolds having become a monopoly rent.

130. Furthermore, CDK and Reynolds have imposed these increased fees on vendors – most of which are passed on to dealers through the price they pay to vendors for software applications – without providing any offsetting price break to the dealers themselves on DMS service. On the contrary, as explained below, the prices that the duopolists charge for DMS

---

<sup>30</sup> DrivingSalesNews, *The Hidden Data Tax That Dealers Don’t Know They Are Paying*, Driving Sales (Oct. 17, 2013).

service rises each year – at a rate much higher than inflation – without any cost justification. This unchecked ability to raise prices both directly and indirectly is evidence of Defendants’ market power.

**III. The Evidence of Defendants’ Agreement to Eliminate Competition in the Dealer Data Integration Market and the Single-Brand Aftermarkets Is Overwhelming**

131. Described in more detail below are Defendants’ (1) February 2015 market division agreement pursuant to which they agreed not to compete in the Dealer Data Integration Market and single-brand aftermarkets; (2) exclusive dealing provisions they have jointly imposed on dealers and vendors; and (3) coordinated campaign to block independent data integrators like Authenticom.

**A. CDK and Reynolds Entered into a Per Se Illegal Written Agreement Dividing the Dealer Data Integration Market and Single-Brand Aftermarkets**

132. As described above, for over a decade, CDK had provided data integration services for dealers using the Reynolds DMS, competing directly with Reynolds’ own RCI integration product. Effective February 18, 2015, however, CDK and Reynolds entered into a written agreement categorized as a “Wind Down Access Agreement” whereby Defendants agreed that they would no longer compete in the Dealer Data Integration Market. It is a classic case of illegal market division: CDK agreed that it would no longer compete in providing access to dealer data on the Reynolds DMS, ceding that ground exclusively to Reynolds. Moreover, because Reynolds already did not compete with CDK in providing access to data for dealers using the CDK DMS, the agreement ensured that CDK and Reynolds would be the exclusive providers of data integration services for dealer data on their respective DMS platforms.

133. More than that, the agreement mandated coordination between the erstwhile competitors in transitioning all of CDK’s vendor clients (i.e., those vendors for whom CDK provided access to dealer data on the Reynolds DMS) into the Reynolds RCI program. In short,

the written agreement is direct evidence of CDK's and Reynolds' collusion in furtherance of their conspiracy to eliminate competition in the Dealer Data Integration Market, and therefore be the sole providers of data integration services for dealers using their respective DMS platforms. With this agreement, Defendants took a key step in eliminating competition from the market.

**1. The Agreement Contains Specific Provisions Dividing the Dealer Data Integration Market**

134. The agreement's key provision states that CDK [REDACTED]  
[REDACTED]  
[REDACTED],” which includes CDK subsidiaries Digital Motorworks and IntegraLink. *See* § 4.1. In short, CDK agreed to no longer provide any “[REDACTED]  
[REDACTED], thereby cementing the conspiracy to divide the data integration market between CDK and Reynolds. *Id.*; Recitals ¶ 2.

135. The agreement granted CDK a “Wind Down Period” of one year to stop pulling dealer data stored on the Reynolds DMS. During that period, [REDACTED]  
[REDACTED].<sup>31</sup> But during that wind-down period, CDK agreed that it would not “[REDACTED]  
[REDACTED].” *Id.*

**2. The Agreement Required Coordination in Transitioning Vendor Clients from CDK to Reynolds**

136. Because CDK agreed that it would no longer provide vendors with data from dealers using the Reynolds DMS, CDK and Reynolds agreed that they would work together to

---

<sup>31</sup> *See* § 3.3 ([REDACTED]  
[REDACTED]  
[REDACTED]).

transition those vendors into the Reynolds RCI program. Specifically, the agreement mandated that CDK “ [REDACTED]

[REDACTED].” *Id.* § 3.1. The agreement went even further and required

CDK to “ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].” *Id.* § 3.4.

137. The fact that CDK and Reynolds agreed to coordinate in transitioning CDK vendor customers to Reynolds lays bare a primary purpose behind the agreement: preventing vendors from using competing data integrators and forcing them to become members of the RCI and 3PA programs.

138. In connection with coordinating the transition of vendors from CDK’s data pulling services into the RCI program, the wind down agreement required CDK to give Reynolds

[REDACTED]

[REDACTED].<sup>32</sup> Absent

an agreement not to compete for each other’s customers, CDK would treat such highly confidential customer information as a trade secret; it would not share it with Reynolds.

---

<sup>32</sup> The customer information CDK gave to Reynolds included the following:

[REDACTED]

” *See* Agreement § 3.3 and Exhibit A.

### 3. CDK and Reynolds Implemented the Agreement

139. Consistent with their agreement, CDK stopped providing dealer data integration services with respect to Reynolds DMS dealers after the wind-down period.

140. Also consistent with their agreement, CDK and Reynolds coordinated the transition of vendors from CDK to Reynolds. On March 2, 2015, CDK sent a letter to its vendor clients – i.e., the ones for whom CDK had pulled data from the Reynolds DMS – announcing that the vendors “will be provided with a roadmap to transition to the Reynolds Certified Interface (RCI) program without any further risk of interruption to existing services.” CDK explained that “we are in a transition period to allow time for [Digital Motorworks] clients to enroll in the RCI program in support of your R&R dealers,” and that “we will assist you to facilitate a smooth transition.” The letter noted that Reynolds had “agreed to protect the current [Digital Motorworks] process for collecting data from R&R dealers during this transition” and promised “a more detailed letter within the next couple of weeks that outlines the transition process.”

141. On April 1, 2015, CDK sent that promised follow-up letter to its vendor customers. The letter begins: “As announced earlier this month, the recent business agreement between CDK Global and The Reynolds and Reynolds Company (R&R) provides for the clients of Digital Motorworks, Inc. (DMI) a streamlined process to enroll in the Reynolds Certified Interface (RCI) program for their R&R dealers. We are now in the transition period to allow sufficient time for this enrollment, and R&R has agreed to provide a grace period for the existing DMI process for R&R data collection during this time.”

142. The letter gave a deadline by when the vendors needed to enroll in the RCI program: “Your deadline for RCI Certification, listed above, refers to when you need to be RCI Certified and the R&R grace period is schedule to end. R&R is ready to assist you with your

transition to the RCI process.” Not only would Reynolds assist them, but so would CDK: “If you would prefer assistance, just let me know, and I will be happy to schedule and participate in an introductory conference call on your behalf.”

143. CDK’s letter then made the sales pitch for RCI participation: “We are pleased to be working with R&R to bring you this streamlined, supported process for handling dealership data for your R&R dealers.” In relation to CDK’s agreement not to compete, the letter stated that if the vendor was “not RCI Certified, it will be more difficult to reliably receive dealership data since DMI is no longer extracting data directly from Reynolds systems.”

144. Remarkably – and putting the lie to “security” concerns with the use of third-party data integrators – the market division agreement still allowed Digital Motorworks to pull data from the Reynolds DMS *so long as* the vendors paid Reynolds first by enrolling in the RCI program. Referring to Digital Motorworks as a “technical agent” in this scenario, the letter explained that “DMI will be able to receive data directly from R&R on your behalf through the RCI program. You will continue to receive the benefits of our data cleansing, standardization, integration and related support services.” This demonstrates that the RCI program (like the 3PA program) reflects no legitimate security concern: so long as vendors pay Reynolds’ exorbitant price for the data, vendors can still use other data integrators for the same services.

145. CDK ended the letter by noting that it had successfully “transitioned clients to the RCI program in the past, and it has proven to be a successful approach to consistent, reliable data extraction.” With respect to how “this new approach differ[ed] from the previous one,” the letter stated: “Prior to this agreement, DMI would extract data directly from its R&R dealers, however there was no guarantee that the data wouldn’t be interrupted during the data extraction process . .

. . With the RCI program, the data is pushed from the DMS through a certified interface,” which CDK claimed made “the process more reliable and consistent.”

146. Reynolds followed up with its own letters to CDK’s vendor clients as the erstwhile competitors transitioned customers from CDK to Reynolds.

147. The agreement had its intended effect: vendors were forced from Digital Motorworks’ and IntegraLink’s data integration services into the Reynolds RCI program. With the switch, vendors now pay far higher prices for the same services.

148. The market division agreement had a direct impact on Authenticom. Not only is the agreement part of Defendants’ overarching aim to eliminate competition, but during the “wind-down” period, Authenticom lost many customers to Digital Motorworks (i.e., CDK). Many vendors decided to leave Authenticom (which was being blocked) and to join CDK (which was not being blocked) on an interim basis, even if those vendors knew they would ultimately be forced into the RCI program. In fact, this was one of Defendants’ purposes for entering into the non-compete agreement: to cooperate in driving vendors away from Authenticom.

**B. CDK and Reynolds Require Dealers and Vendors to Enter into Exclusive Dealing Arrangements That Are Patently Anticompetitive**

149. In their market division agreement, CDK and Reynolds agreed not to compete in the Dealer Data Integration Market. But to remove the rest of the competition, further measures were required. Accordingly, CDK and Reynolds imposed exclusive dealing provisions in dealer contracts (dealers cannot provide access to their data to anyone else) and vendor contracts (vendors cannot obtain dealer data from anyone else). For independent data integrators like Authenticom, these exclusive dealing provisions have foreclosed the entire data integration market for dealers using the CDK and Reynolds DMS platforms.



**1. Defendants' DMS Contracts with Dealers Grant Defendants an Exclusive Right to Access the Dealers' Data**

**a. The Dealer Exclusive Dealing Terms**

150. In their DMS contracts with dealers, both CDK and Reynolds require dealers to agree that they will not provide anyone other than the DMS provider access to their data for purposes of data integration and syndication to vendors. The contractual terms thus prohibit dealers from granting access to their data to anyone else, including data integrators such as Authenticom.

151. CDK's current standard DMS contract contains an explicit exclusive dealing provision that forecloses dealers from using other integration providers, including Authenticom: "[REDACTED]." Master Services Agreement § 6.D. It also states: "[REDACTED]". *Id.* at § 6.B. While the agreement bars dealers from granting data access to third parties, the agreement expressly provides that CDK is able to access the data for purposes of data integration and syndication. These provisions last the life of the DMS contract, which is a minimum of five years. Together, these provisions give CDK an exclusive right to access dealer data on the CDK DMS for purposes of data integration and syndication. And because data integration providers depend on dealer authorization to access the dealers' data, these provisions effectively foreclose any competitor from competing with CDK in the provision of data integration services for dealers whose data is stored on CDK's DMS database.

152. Reynolds also has the same provisions in its current standard DMS contract. It prohibits dealers from "[REDACTED]." Master Agreement § 1. The Reynolds DMS Customer Guide, which is incorporated into the contract,



similarly states that the dealer is barred from “[REDACTED]” the DMS. *See* Customer Guide at p. 21. Reynolds has interpreted these provisions to mean that dealers cannot grant access to their own data on the DMS database. Like the CDK dealer contract, the Reynolds contract explicitly gives Reynolds the right “[REDACTED] [REDACTED] [REDACTED].” *Id.* at pp. 8-9. These rights and restrictions last as long as the DMS contract, typically five to seven years. As with the CDK contract, together these provisions give Reynolds an exclusive right to access dealer data on the Reynolds DMS for purposes of data integration and syndication, to the exclusion of all others.

**b. CDK and Reynolds Vigorously Enforce the Dealer Exclusive Dealing Provisions**

153. CDK and Reynolds vigilantly enforce the restrictive terms in their DMS contracts. As detailed throughout this complaint, CDK and Reynolds block other data integrators from accessing dealer data. *See infra* Part III.C.4.

154. These provisions are harmful to dealers, yet CDK and Reynolds are able to force dealers to agree to them because of their market power in the DMS Market. Many dealers do not even realize that CDK and Reynolds have inserted the exclusive dealing provisions into the DMS contracts. Dealers complain often, but to no avail. For example, after CDK disabled Authenticom’s login credentials, one dealer protested to CDK: “You do not have our authorization to disable user accounts. It is my data and I decide who has access to it.” CDK responded that it in fact had the right to control access. The dealer asked for “documentation validating CDK is allowed to disable OUR accounts to OUR data without OUR permission.” CDK responded that the DMS Agreement “contains language stating that unauthorized access to the DMS is prohibited,” citing the provisions quoted above.

155. More recently, CDK added the following warning shot to dealers on its dealer login page: “Please be advised that the creation of User IDs for use by unauthorized third parties violates the terms of your CDK [DMS] Agreement.”

156. Reynolds has taken the extra step of not only disabling login credentials, but actually filing lawsuits against competing data integrators for tortious interference with the DMS contracts. *See supra* Part I.A.2. Reynolds regularly hangs this same threat over Authenticom. For example, on April 6, 2015 – shortly after Reynolds and CDK entered into their market division agreement – Mr. Schaefer (one of Reynolds’ senior executives involved in forging the agreement) sent a letter to Authenticom threatening that “any knowing attempt by Authenticom to induce Reynolds dealers to allow such third party access . . . gives rise to liability on the part of Authenticom for, among other things, tortious interference with contracts.”

**2. Defendants’ Contracts with Vendors Grant Defendants an Exclusive Right to Provide Data to Vendors**

157. In addition to inserting exclusive dealing provisions in their dealer contracts, CDK and Reynolds have also inserted exclusive dealing provision provisions in their data integration contracts with vendors. As a result, a vendor using CDK or Reynolds for data integration services must agree *only* to use CDK or Reynolds, and forgo using anyone else.

158. Specifically, the CDK 3PA and the Reynolds RCI contracts contain exclusive dealing provisions that prohibit vendors from obtaining dealer data from anyone other than CDK (through the 3PA program) or Reynolds (through the RCI program). Thus, if a vendor obtains dealer data through the 3PA program (for CDK dealers) or the Reynolds RCI program (for Reynolds dealers), the vendor is barred from obtaining the dealer data from any other integrator. These exclusive dealing provisions foreclose Authenticom from its entire customer base.

**a. The Vendor Exclusive Dealing Terms**

159. CDK. The current CDK 3PA contract states: “[REDACTED]  
[REDACTED]  
[REDACTED].” See CDK 3PA Contract § 2(e); § 1(a)(l). The contract goes on to state that the vendor cannot “[REDACTED]  
[REDACTED].” *Id.* That specifically prohibits vendors from having Authenticom (or any other data access provider or even the dealer itself) provide the data to the vendor.<sup>33</sup> Moreover, the exclusivity provision applies to every software application a vendor has. Thus, if a vendor uses CDK’s integration product for one application, the vendor must then use CDK for every other application too.

160. The penalty for accessing dealer data other than through CDK is termination. “[REDACTED]  
[REDACTED].” *Id.* § 6(g).

161. These exclusive terms purportedly *last forever*. The contract states: “[REDACTED]  
[REDACTED].” *Id.* § 6(j) (emphasis added). By extending the life of the prohibitions into perpetuity, the contract ties the vendor to the 3PA program indefinitely. Even if the vendor were no longer to participate in the 3PA program, it would still be barred – forever – from obtaining data from any CDK dealer from any other source. That gives CDK carte blanche to abuse vendors and raise prices once they enter the 3PA program, because few, if any, vendors

---

<sup>33</sup> If a vendor should breach the contract and obtain data from a source other than CDK, the vendor will not only be liable for breach of contract, but the vendor must “[REDACTED]  
[REDACTED].” See CDK 3PA Contract § 2(e).



the data access fees in any way, whether directly or indirectly, even though the data access fees are often passed down to dealers in the form of higher vendor prices.

167. The CDK 3PA contract states that vendors “[REDACTED]”  
[REDACTED]  
[REDACTED]  
[REDACTED].” CDK  
3PA Contract § 10.

168. The CDK contract also bars vendors from indicating “[REDACTED]” that an increase in the price of their own services is related to an increase in the data access fees charged by CDK. The language is sweeping: “[REDACTED]”  
[REDACTED]  
[REDACTED]  
[REDACTED].” *Id.*

169. Similarly, the Reynolds RCI contract prohibits vendors from disclosing any terms or conditions of the contract – including the pricing paid for the data integration services – to any party, including dealers. *See* RCI Contract § 2.7.

170. Through these provisions, CDK and Reynolds make it exceedingly difficult, if not impossible, for dealers to understand the true cost of DMS services (given that dealers ultimately bear the cost of the data access fees imposed by CDK and Reynolds). By shrouding in secrecy the source of data-related price increases, CDK and Reynolds thwart competition and transparency in the DMS Market.

**c. CDK and Reynolds Vigorously Enforce the Vendor Exclusive Dealing and Price Secrecy Provisions**

171. Like the exclusive dealing provisions in the dealer contracts, CDK and Reynolds aggressively enforce the exclusive dealing provisions against vendors. They punish vendors that obtain dealer data from any other integrator, impose large fines, threaten to cancel the vendor's contract, and initiate audits.

172. A prime example involves a large vendor of customer relationship management software. In August 2016, Reynolds sent a letter to the vendor stating that it had "come to Reynolds' attention that [the vendor] has materially breached the Agreement by violating, without limitation, the Agreement's prohibition against Non-Approved Access and/or Non-Approved Use" by obtaining dealer data from Authenticom. "More specifically," the letter explained, "Reynolds recently received documentary evidence from one of our mutual dealership customers showing that [the vendor] is flagrantly violating the above provisions by using an unauthorized, third-party data broker to extract data" for one of the vendor's applications. Reynolds threatened to terminate the RCI agreement with the vendor unless the vendor agreed to "immediately cease and desist" from using dealer data extracted "using a non-RCI method (e.g., using Authenticom/DealerVault software)." Reynolds demanded that the vendor "submit to a third-party audit (at [the vendor's] expense) . . . to verify that all instances of the use of non-RCI data extraction have been reported and addressed." Reynolds also demanded "a one-time payment to Reynolds of [REDACTED]" under the agreement's liquidated damages clause. Reynolds threatened that the [REDACTED] figure was "offered in the spirit of compromise" and if the vendor did not accede to the demands in the letter, "Reynolds intends to establish that [the vendor's] conduct constitutes multiple breaches for purposes of the Agreement and that Reynolds is

entitled to far greater amount in damages.” Significantly, nothing in the letter was about security – Reynolds just wanted its fees and the vendor to stop using Authenticom.

173. Such strong-arm tactics are typical of Reynolds and CDK, and they have succeeded in intimidating vendors. Indeed, the vendor in the above example not only terminated its relationship with Authenticom, but it was so worried about running afoul of Reynolds again that it asked Authenticom, as a preventative measure, to disregard any future request to provide data in case the vendor inadvertently tried to rely on Authenticom’s services again.

174. CDK and Reynolds also strictly enforce the Price Secrecy Provisions with an iron fist. They have threatened numerous vendors with claims of material breach and liquidated damages for so much as mentioning that they pay large data access fees.

### **3. The Dealer and Vendor Exclusive Dealing and Price Secrecy Provisions Are Anticompetitive**

175. The exclusive dealing provisions in Defendants’ dealer and vendor contracts are anticompetitive. They are per se illegal because they are part of Defendants’ agreement to eliminate competition in the primary Dealer Data Integration Market and secondary aftermarkets. They are also anticompetitive and invalid under the rule of reason. They foreclose a substantial percentage of the integration market – given CDK’s and Reynolds’ market share in the DMS Market, at least 75 percent of the nation’s dealers are prohibited from using Authenticom for automated integration services. When considered in light of the aftermarkets, 100 percent of dealers using the CDK or Reynolds DMS systems are prohibited for using Authenticom. From the perspective of vendors, the foreclosure is even more extreme. If a vendor uses CDK as an integrator for even a single CDK dealer, that vendor may no longer use Authenticom as an integrator for *any* CDK dealer, and the same is true for Reynolds. There are few, if any, vendors

that could survive without serving CDK and Reynolds dealers, and therefore the vast majority of vendors are foreclosed from using Authenticom.

176. The serious anticompetitive effects of Defendants' conduct on the Dealer Data Integration Market and respective aftermarkets – and the widespread harm to dealers and vendors – is established by the massive price increases Defendants have successfully imposed, *see infra* Part IV.A. Similarly, the price secrecy provisions make it difficult, if not impossible, for dealers to understand the true cost of using either CDK or Reynolds for DMS services. Defendants have also demonstrated an ability to exclude their rivals, having eliminated all competition in the integration market except for Authenticom, which has suffered serious financial injury. Given Defendants' market power and leverage, dealers and vendors had no choice but to enter into the exclusive dealing terms, *see supra* Parts I.B; III.B.1. The presence of coercion is also demonstrated by Defendants' blocking of all other competitors.

177. The impact of the exclusive dealing provisions is amplified by their lengthy duration. Defendants' DMS contracts with dealers typically last five to seven years. Reynolds' contracts with vendors are typically 3 years with automatic renewals. And CDK's exclusive dealing terms with vendors purport to be indefinite and non-terminable.

**C. Defendants Are Engaged in a Coordinated Campaign to Block Authenticom's Access to Dealer Data and Thereby Destroy Its Business**

178. Having succeeded in eliminating the rest of the competition, CDK and Reynolds have now stepped up their coordinated attacks on Authenticom by blocking its access to dealer data (despite dealer authorization). Through this group boycott, Defendants are intent on destroying Authenticom's business.



**1. Defendants Have Admitted That They Have Agreed to Restrict Access and Block Authenticom**

179. Senior CDK and Reynolds executives – including those who formed and implemented the agreement – have admitted that CDK and Reynolds have entered into an agreement to restrict access to dealer data on their systems and to destroy data integrators like Authenticom.

180. Specifically, on April 3, 2016, at an industry convention, Dan McCray (CDK's Vice President of Product Management) approached Mr. Cottrell and said that they should "take a walk." Mr. McCray led Mr. Cottrell off the convention floor and down a service ramp to a secluded area. Mr. McCray then confirmed the existence of the illegal agreement, stating that CDK and Reynolds had agreed to "lock you and the other third parties out." In reference to a prior offer by CDK to acquire Authenticom's business for \$15 million, Mr. McCray confirmed the illegal agreement again, stating that the number was so low because Authenticom's "book of Reynolds business is worthless to us because of the agreement between CDK and Reynolds." Mr. McCray then grew threatening: "I wanted to look you in the eye and let you know man to man, I have been mandated by our new CEO to seek you out and destroy your business on our systems." Referring to the exclusive dealing provisions in the dealer DMS contracts, he stated that "we will enforce our contract with dealers and sue them if needed to keep you out of our systems." "For god's sake," he concluded, "you have built a great little business, get something for it before it is destroyed otherwise *I will f\*\*\*ing destroy it.*" Mr. Cottrell rejected Mr. McCray's threats, refused to sell his company for a fraction of its value, and insisted Authenticom would continue to serve its dealer and vendor customers.

181. Top Reynolds executives have delivered the same message. In May 2015, Mr. Schaefer – Reynolds' head of data services and one of the architects of the conspiracy – told Mr.

Cottrell during a phone conversation that CDK and Reynolds had an agreement to support each other's 3PA and RCI programs and therefore block competitors like Authenticom from pulling dealer data. Mr. Brockman was adamant, Mr. Schaefer said, that all third-party data integrators must be cut off. Mr. Schaefer also said that he was in communications with other DMS companies to try to convince them to join CDK and Reynolds in the agreement to block independent data integrators. To date, he has not had success – every other DMS company recognizes a dealer's right to have Authenticom (and others like CDK-owned Digital Motorworks and IntegraLink) provide data integration services.

**2. Defendants' Employees Are Working In Concert to Coordinate the Blocking of Authenticom**

182. CDK and Reynolds have not only agreed to block Authenticom, but they have employees actively working together to coordinate the technical aspects of that blocking.

183. In December 2016, during one particular vendor's discussions with CDK about joining the 3PA program and leaving Authenticom, Steve French – CDK's senior director of client and data services – told the vendor that a large portion of his job was to work with Reynolds to ensure third-party data integrators like Authenticom remain locked out. Mr. French suggested that resistance to getting dealer data from CDK and Reynolds was futile as they were working together to lock out third party data integrators like Authenticom.. Mr. French's background makes him an ideal liaison between CDK and Reynolds: he previously worked for Reynolds as its data collection manager.

**3. Defendants Tried to Coerce Authenticom to Exit the Dealer Data Integration Market**

184. CDK and Reynolds have tried multiple times to coerce Authenticom to exit the Dealer Data Integration Market and cede the field completely to them. As already recounted

above, CDK told Mr. Cottrell that he should sell his business to CDK for \$15 million because otherwise CDK and Reynolds were going to destroy it.

185. Reynolds has also given Authenticom an ultimatum to exit the data integration market or face escalating attacks on its business. As noted above, in April 2015, Reynolds threatened to sue Authenticom for tortious interference. Authenticom rejected the threat, and in response noted that “a significant percentage of R&R’s [dealer] customers also are Authenticom’s customers” and, like Reynolds, Authenticom and the dealers “have contractual agreements.” In response, on May 7, 2015, Reynolds’ lawyer sent Mr. Cottrell a proposed “Wind Down” agreement. Authenticom would shut down its data integration business and, in exchange, Reynolds would stop blocking Authenticom’s access to dealer data during the one-year wind down period. During that so-called “grace” period, Authenticom would be required to transition Authenticom’s vendor clients into the RCI program, where they would pay Reynolds’ vastly higher integration fees. Mr. Schaefer told Mr. Cottrell that the draft agreement Reynolds provided was word-for-word what Reynolds and CDK had agreed to just months earlier. In fact, the attorney that sent the Wind Down agreement is the same Reynolds lawyer who had negotiated Reynolds’ market division agreement with CDK.

186. Mr. Cottrell rejected Reynolds’ threats. As he wrote to Mr. Schaefer, instead of leaving the market, Authenticom was intent on providing “a safe and secure data movement option in a fair and competitive marketplace.”

#### **4. Defendants Are Blocking Authenticom’s Ability to Provide Dealer Data Integration Services**

187. Having failed to convince Authenticom to exit the data integration market on its own, CDK and Reynolds have waged an all-out assault on Authenticom by intensifying their blocking activities. Vendors – with no choice given the interruptions to their services – have left

Authenticom and joined the 3PA and RCI programs, putting Authenticom's business into a downward spiral.

**a. CDK and Reynolds Have Disabled Authenticom's Usernames En Masse**

188. On August 1, 2016, Authenticom's employees walked into work and confronted a business catastrophe. Overnight, CDK had disabled Authenticom's login credentials at thousands of dealerships. A throng of dealers and vendors called Authenticom, frantically trying to find a way to re-establish Authenticom's connection and resume the flow of data. Vendors and dealers alike had their business operations interrupted. Over the ensuing weeks and months, CDK unleashed wave after wave of blocking actions that disabled Authenticom's login credentials for thousands of dealerships. In terms of timing, CDK has informed dealers that "[o]ur goal is to complete the removal" of "unauthorized third-party access methods by December 31, 2016." CDK then promised that in 2017 it would "further increase our security actions to prevent the use of unapproved data access methods."

189. Reynolds' blocking tactics started earlier and have been more sustained than CDK's, as CDK did not start blocking independent data integrators until it entered into the agreement with Reynolds in 2015. Reynolds first started disabling Authenticom's usernames in 2009 when it introduced gimmicks such as "challenge questions" and "captcha" (where the user has to enter random blurred text) to make it more difficult to automate the pulling of data. Reynolds also targeted Authenticom's usernames for specific vendors, disrupting the data flow for those vendors and thereby forcing them to join the RCI program. In June 2013, Reynolds intensified its tactics by disabling Authenticom's usernames en masse. "Effective immediately," Reynolds announced to its dealers, "Reynolds will begin the rollout of prohibiting automated access into" its DMS. "This will impact any process that is set up to directly access [the DMS]

without any manual intervention.” Over a three-month period in the summer of 2013, Reynolds disabled 27,000 profiles used by Authenticom at over 3,600 dealers. Reynolds’ actions resulted in an almost complete collapse of Authenticom’s integration business for dealer data for dealers using the Reynolds DMS.

**b. Dealers Have Protested to CDK and Reynolds and Demanded That They Stop Blocking Authenticom**

190. Dealers have demanded that CDK and Reynolds stop blocking Authenticom. The dealers have made clear that the data is theirs, that they control access to it, and that the disabling of Authenticom has interrupted their operations and caused economic harm. But CDK and Reynolds have rejected the dealers’ objections.

191. The dealer complaints are too numerous to fully recount here. But a few examples make the point. In November 2016, one Mercedes dealership in California wrote to CDK: “When will you stop the blocking of our user profiles? This must stop.” The dealer decried CDK’s “attempt to stop all other data access routes thereby forcing us to use [CDK’s] data monetizing scheme if we want to access our data.” As the dealer recognized, the blocking of Authenticom was an effort to obtain the economic benefits of the dealers’ data. “When will CDK stop trying to monetize data owned by [us] at our expense? All being orchestrated under the guise of ‘protecting our data.’ Frankly most can see right through this propaganda smoke screen. The data could be protected by using available technology that doesn’t cut off the dealers’ access to their own data using fully automated routines.” The dealer explained that because of CDK’s exorbitant data access fees, it could not use the applications it wanted: “We would like to purchase the XTime application. The CDK data access charges make that option prohibitively expensive. Did CDK actually think that these exorbitant data access charges levied against our third party solution providers would not get passed directly back to us?”

192. One Virginia dealer asked his employees “to raise holy hell with CDK. This is really affecting our business.” A Wisconsin dealer explained that it had even created a login for the owner of the dealership “to see if CDK had the nerve to deactivate it. They did! I have very strongly voiced by phone to my CDK rep to STOP IT.” A Lexus dealer in Ohio related that it had “lit into [CDK] about how CDK is making it more difficult for me now with this agenda of theirs (I even mentioned Authenticom’s name and how I felt they were being unfairly singled out to frighten dealers regarding their DMS security).”

193. Dealers explained that they preferred the superior product and service they received from Authenticom. For example, a Lexus dealership in California wrote that “[a]s a dealership owner, I believe that CDK has no right to deny me access to my own data. By extension, I also retain my rights to distribute my data to chosen vendors who meet my strict criteria for data security.” Praising Authenticom’s product, the dealer wrote that “with each vendor requiring different kinds of data extraction, I feel it would be far more effective to support Authenticom and DealerVault, to build a great single point of extracted data, and plug my vendors into their ecosystem.”

194. One final example comes from a Ford dealership in Wisconsin: “I have been very vocal to my CDK rep in terms of who owns the data and how their disruption of our business is costing us money in potential lost sales with our vehicle inventory not being up to date.” Like most dealerships, however, it felt trapped between CDK and Reynolds, given the DMS needs of their business. “The only [DMS providers] we are comfortable handling this business, unfortunately for us, is CDK and R&R.” And that, in a nutshell, is the dilemma dealers face: no matter which DMS provider the dealer selects, both CDK and Reynolds have agreed to block independent data integrators and have seized control over access to the dealer’s own data.

**c. Dealers Have Set Up New Usernames for Authenticom, but Those Have Been Quickly Blocked by CDK and Reynolds Too**

195. After CDK and Reynolds disabled the dealer-created Authenticom credentials, dealers worked cooperatively with Authenticom to set up new credentials and reestablish access. Given the sheer scale of the mass blocking, Authenticom was forced to redirect a majority of its 120-person workforce to the effort – including at one point hiring 50 temporary employees solely to help dealers navigate around the shutdowns. But as soon as dealers set up new login credentials, CDK and Reynolds disabled them. Dealers understandably grew weary of devoting time and energy to setting up new usernames day after day, particularly given the interruptions to their operations that the blocking of data was already causing.

196. Among the many examples, one Nissan dealership from Indiana reported that it had “updated a few profiles and within 24 hours they are locked out again.” A Delaware dealer called “CDK and yelled at them for about 2 hours telling them to let me handle security and to stop touching my user list in every single situation. They refused to stop.”

197. Amid the constant attack on dealer logins, dealerships threw up their hands. “I cannot continue to create new profiles nor does my schedule allow for time to reset this log on daily,” a large California dealership stated. With respect to Reynolds, a large dealership group explained that the “process to recreate a user ID in Reynolds is not as simple as it used to be and now takes approximately 30 min. to remake [Authenticom’s] account with the proper access[;] that is time I don’t have.” The dealer lamented that although it did “like what [Authenticom’s] product does and the ease and control we have,” it could not continue to deal with Reynolds’ repeated disabling. Underscoring the leverage that DMS providers wield, a Massachusetts Ford dealer explained that “[w]e cannot play the nightly cat and mouse game of us enabling the [Authenticom] account – only to have them shut it down. We cannot put our company at risk by

having CDK declare us – not secure – and shutting us out of our own server and making it impossible to do business.”

**d. CDK and Reynolds Have Refused To Give Credence to the Dealers’ Objections**

198. Even though dealers forcefully objected to CDK’s and Reynolds’ blocking of Authenticom, CDK and Reynolds did not listen. Instead, they insisted that, by re-establishing a username for Authenticom, dealers would breach their DMS contracts. For dealers, this is the “nuclear option” – because they simply cannot operate without a functioning DMS.

199. A vendor reported to Authenticom that dealers “are so worried to go against the grain with CDK thanks to very threatening language being used. CDK is telling my dealerships that they risk litigation if they cooperate with enabling profiles.” CDK “told another dealership that enabling profiles violates their agreement with CDK and it could result in aggressive action.” A Toyota Reynolds dealership in California said “it does not matter what ID is used it will trigger the Suspicious Activity triggers according to [Reynolds] and shut down any account used to access Data,” with the takeaway that “this issue will NEVER GO AWAY!” As one Dodge dealer in Texas reported, its CDK “rep said that setting up a new profile would work for a day or two but our account is now being monitored. Basically he told me that they have control and that is the way it’s going to be.”

**e. CDK and Reynolds Are Proactively Contacting Dealers Served by Authenticom to Pressure Them to Have Their Vendors Switch to the RCI and 3PA Programs**

200. In conjunction with disabling Authenticom’s profiles, CDK and Reynolds have contacted dealers to convince them to have their vendors switch to the 3PA and RCI programs. The pattern is familiar: block Authenticom, and then push vendors to switch.



201. On August 22, 2016, Mr. Karp sent a letter to all of CDK's dealers served by Authenticom with the following message: "We are contacting you because your dealership has been identified as a client of a third party that is accessing your data through CDK systems by unauthorized means." He stated that CDK would no longer allow independent data integrators to access dealer data, and that vendors therefore needed to "begin the Third Party Access program application process immediately to avoid disruption." Mr. Karp followed up this letter with repeated communications to dealers throughout the fall of 2016. In letter from September 23, 2016, he told dealers to "[s]hare your list of vendors with us so that our Third Party Access program team can invite vendors who are not already part of the program to join." CDK's goal is plain: ensure that Authenticom has no way to access dealer data and then take Authenticom's customers.

202. Reynolds has delivered the same message with the same goal, repeatedly notifying dealers that it was "prohibiting automated access" to data integrators and following that up with a marketing push: "[I]f a third party vendor you do business with is impacted by this, please refer them to the Reynolds Certified Interface hotline."

**f. CDK and Reynolds Have Spread False Information About Authenticom's Security as Part of Their Marketing Push**

203. As part of their effort to discredit Authenticom and force vendors to join the 3PA and RCI programs, CDK and Reynolds have spread falsehoods about Authenticom's data security.

204. For example, in multiple letters to dealers, Mr. Karp falsely stated that, with Authenticom, "there are no limits on data elements that can be accessed, increasing the risk of misuse. There is also an inability for you to track and monitor where your data is going." These statements are demonstrably false. Authenticom pulls only the data dealers specify, and with

DealerVault, dealers have complete control and visibility over the flow of their data. Mr. Karp also warned of “unauthorized software” being “installed on your CDK DMS system,” which is also false. Authenticom does not install any software on the DMS system, but simply runs data reports just as the dealer can. CDK and Reynolds have also raised the fake concern that “sharing data through intermediaries such as Authenticom increases data handling risks.” CDK does *the exact same thing* (through its Digital Motorworks and IntegraLink subsidiaries) in pulling data as a “data-handling intermediary” and has for years.

205. Defendants’ criticisms of Authenticom’s security ring especially hollow given that they *both use Authenticom for data integration services for their own applications*. For example, Reynolds uses Authenticom to pull data from a handful of *Reynolds’ own dealerships* for use in *Reynolds’ own applications*. Reynolds has turned to Authenticom to pull data for those dealerships – using the standard procedure of login credentials and data scraping – and Authenticom then provides that data to Reynolds for use in its applications. If Defendants succeed in putting Authenticom out of business, then Reynolds will have to start pulling data itself from these Reynolds dealerships.

206. Another example involves AVRS, Inc., a wholly owned joint venture of CDK and Reynolds. AVRS provides electronic registration and titling services for dealers in California, and it uses Authenticom for data integration services. Thus, on behalf of Defendants’ own joint venture, Authenticom pulls data from *CDK dealers* and *Reynolds dealers*. The data AVRS requires is the car buyer’s identification information, including name, address, and date of birth. The state of California mandates security protections for this data; Authenticom complies. AVRS – and thus CDK and Reynolds – would not use Authenticom otherwise.

207. In another example, before it entered into the conspiracy with CDK, Reynolds used Authenticom to pull data from CDK dealers. (Now, post-agreement, Reynolds can no longer use Authenticom for CDK dealers.) But even today, Reynolds still uses Authenticom to pull data from non-CDK and non-Reynolds dealers for use in Reynolds' applications. Reynolds is actually one of Authenticom's larger vendor clients. Again, if Defendants' succeed in driving Authenticom out of business, then Reynolds will have to use CDK (i.e., Digital Motorworks) for integration services for these dealers.

**g. Authenticom Is Losing Its Customers – and Therefore Its Business – Because of Defendants' Actions**

208. CDK's and Reynolds' goal is simple: to put Authenticom out of business, which will cement their monopoly over integration services for dealer data on their systems. It is working. Despite the fact that dealers and vendors prefer Authenticom's better-priced and higher-quality product and services, vendors have had no choice but to leave Authenticom and join the 3PA and RCI programs.

209. "After being a loyal client for over six years," one longtime vendor client of Authenticom wrote, "we are compelled to make a business decision to pursue Third Party Access from CDK Data Services." The vendor could not sustain the business disruptions caused by the blocking. "Over the past 60 days, we have averaged 100 of our dealer clients blocked from DealerVault/Authenticom polling the dealer's data. The effect of these disruptions has taken a serious toll on our dealer business clients causing them to terminate or suspend marketing services with us." Many vendors made the same point about the detrimental effects of Defendants' blocking tactics. "I know this [blocking by CDK and Reynolds] is causing you a great deal of angst and lost sleep I am sure. I support your battle but I need to try and save myself at some point." "Between the Reynolds lockouts and the subsequent CDK lock-outs,"

another vendor explained, “our business has contracted due to dealer cancellations.” Another wrote: “We have (reluctantly) fallen victim to CDK and have already moved several (nearly all) [accounts] to CDK.” The data interruptions cost that vendor “the loss of tens of thousands of dollars that we cannot make up. Ensuring data is complete and flowing properly is essential to our business.” As a result, the vendor saw “no choice but to bite the proverbial bullet and go back to CDK.” Dealerships often delivered the bad news themselves. “Due to major issues with DealerVault’s Reynolds login getting disabled over and over again[,] [w]e need to cancel the account,” a Reynolds dealership in Texas explained. “We now have [the vendor] pulling directly from Reynolds.”

210. Leaving Authenticom was especially frustrating for vendors because they much preferred Authenticom’s superior data integration services to CDK’s and Reynolds’. As one vendor summarized, the “process to onboard data via [Authenticom] is streamlined and much easier for both our company and the individual dealership. Plus, the data accuracy and formatting is very consistent when it is secured (this is not the case when data is pulled directly from CDK).” In the end, the vendor lamented, “the only party that truly suffers here is the actual dealer. It takes us longer to provide them the services they are requesting and have paid for. The data is not as clean, therefore requiring additional processes and data scrubbing and appending tools to be applied on our side. And the costs are greatly increased – literally double – due to the egregious fees that CDK charges.”

#### **IV. Defendants’ Actions Have Harmed Competition**

211. Defendants’ anticompetitive conduct has not just harmed Authenticom, it has harmed competition itself – first and foremost through dramatic price increases, but also through reduced output, degraded product quality, and diminished customer choice. CDK’s and Reynolds’ anticompetitive conduct has harmed dealers, vendors, and the industry as a whole.

**A. Defendants' Anticompetitive Conduct Has Resulted in Massive Price Increases in the Dealer Data Integration Market**

212. Having eliminated their competitors, CDK and Reynolds have exercised their market power and imposed enormous price increases on data integration services. Neither vendors nor dealers have been able to stop or resist these increases.

213. There are two ways to look at the price increases: (1) the price difference between what Authenticom (and other independent data integrators) charged and what CDK and Reynolds now charge the same vendors for the same services; and (2) the price difference between what CDK and Reynolds charged before they entered their illegal agreement and enhanced their market power, and what they charge now. Under both measurements, the price increases have been immense.

**1. CDK and Reynolds Have Imposed Massive Price Increases As Compared to What Authenticom Charged**

214. Data integrators charge vendors per dealership rooftop, sometimes referred to as a "connection." Thus, if a dealer has ten rooftops (i.e., ten individual franchises), then the vendor would need ten separate connections for that dealer. To pull data, Authenticom has consistently charged vendors \$25 for one data feed and \$50 for two or more (up to seven). On average, Authenticom charges vendors between \$30 and \$40 a month per connection. For bi-directional access to dealer data, Authenticom has generally charged \$75 per connection. Other independent data integrators charged similar rates. For example, between 2008 and 2016, SIS charged around \$40 per connection for pulling data and \$70 per connection for bi-directional access (until it was forced out of the data integration market).

215. CDK and Reynolds now charge far higher rates than those charged by Authenticom and former data integrators. One prominent vendor paid Authenticom \$35 per month to pull data; when it was forced to join the RCI program for data integration services, the

monthly rate charged by Reynolds was \$210, a 500 percent increase. Another large vendor purchased data integration services from SIS for years, at a rate of \$45 to \$50 per month. That vendor now pays Reynolds and CDK monthly charges of between \$300 and \$866 (Reynolds) and between \$300 and \$700 (CDK).

216. In addition to these monthly fees, CDK and Reynolds also charge vendors enormous upfront fees to initiate services. CDK and Reynolds charge at least \$30,000 to join the 3PA and RCI programs, with “setup” fees of around \$300 (or more) per connection. These initiation fees are much more than anything charged by Authenticom and other independent data integrators. For example, Authenticom collects an upfront fee of \$2,500, but that fee is credited against the first invoices. Moreover, Authenticom does not charge an additional per-connection setup fee as CDK and Reynolds do.

**2. CDK and Reynolds Have Dramatically Increased the Prices for Their Own Data Integration Services**

217. CDK and Reynolds dramatically raised their data integration fees upon entering into their conspiracy in February 2015 to divide the market and coordinate their efforts to block Authenticom and other independent data integrators.

218. Before entering the agreement with Reynolds in February 2015, CDK charged an average of \$70 per connection. Since 2015, the average cost per connection has risen to at least \$250 to \$300 (and often much more). This constitutes, at the conservative end, an increase in the range of 250 to 325 percent in the price of data integration services.

219. CDK’s prices for the 3PA program stand in stark contrast to the prices CDK charges for data access to non-CDK dealers. Today, CDK (through Digital Motorworks and IntegraLink) charges between \$25 and \$50 per connection to non-CDK dealers, while it charges on average between \$250 and \$300 for the same services to CDK dealers.

220. As for Reynolds, before 2010, Reynolds generally charged vendors less than \$100 per month per connection. By 2013 – after it had begun to block independent data integrators and impose (and enforce) exclusivity provisions in its contracts with dealers and vendors – Reynolds raised its monthly prices per connection from less than \$100 to between \$300 and \$500. This constitutes a price increase in the range of 200 to 400 percent in the price of data integration services. And since Defendants entered the agreement in 2015, Reynolds has been raising its prices for data integration services even more, including by charging many vendors a transaction charge for every data pull. CDK has instituted the same practice of charging some vendors an additional per-transaction fee on top of their already large monthly fees.

### **3. The Evidence of CDK’s and Reynolds’ Price Increases Is Overwhelming**

221. Leading industry publications have reported widely on the price increases imposed by CDK and Reynolds on data integration services.

222. In July 2015, shortly after CDK and Reynolds entered their agreement, *Automotive News* reported that “CDK said it intends to charge each third-party vendor . . . between \$250 and \$300 a month per store for each software product. The current fees average about \$70 per software product.”<sup>34</sup> Another “vendor executive said the new program would raise monthly data fees from about \$50 per store per month today to as much as \$600 for customer relationship management software.” *Id.* As for Reynolds, “[p]articipation costs one CRM vendor more than \$700 a month per Reynolds store. The vendor requested anonymity because Reynolds has strict nondisclosure provisions in its vendor contracts.” *Id.*

---

<sup>34</sup> David Barkholz, *Dealers Will Pay Up for Vendors’ Data Access After CDK Switch*, *Automotive News* (July 20, 2015).

223. Other publications reported similarly. “According to numerous vendors I’ve talked with,” The Banks Report wrote in October 2015, “prices to access data in CDK’s systems under the new initiative could increase anywhere from 300% to 800%.”<sup>35</sup> In the face of such massive price increases, “[d]ealers are caught in the middle – either they’ll end up seeing increased charges from their vendors or, they’ll see a sudden drop off in service from their vendors.” *Id.* In February 2017, The Banks Report provided an update, noting that “vendors complain the pricing is creating an untenable situation in the industry. Two separate vendors shared with TBR during the recent NADA convention that they each pay a combined \$30 million to CDK and Reynolds for access rights.”<sup>36</sup> One dealer – Friendship Enterprises from Bristol, Tennessee – told *Automotive News* in December 2016 that, as a result of “CDK’s data surcharge,” it has large “overhead [expenses] now that we shouldn’t have. It’s our data.”<sup>37</sup>

#### **4. CDK and Reynolds Continue to Charge Dealers Escalating Fees for DMS Services**

224. As described above, because vendors cannot absorb the massive price increases imposed by CDK and Reynolds, vendors pass most if not all the increased data integration fees down to dealers. At the same time, and despite this new source of revenue, CDK and Reynolds have done nothing to reduce fees for DMS services. On the contrary, CDK and Reynolds ratchet up the DMS fees year after year, with no price break to dealers to make up for the pass-through costs for data integration.

225. Both CDK and Reynolds have fee escalation clauses in their DMS contracts with dealers. The standard Reynolds contract provides that DMS fees go up every year on March 1.

---

<sup>35</sup> Cliff Banks, *Data Access Battle Goes Nuclear*, The Banks Report (Oct. 12, 2015).

<sup>36</sup> Cliff Banks, *CDK, Reynolds and Reynolds Sued for Alleged Antitrust Practices*, The Banks Report (Feb. 4, 2017).

<sup>37</sup> Vince Bond Jr., “*Held Hostage*”: Dealer’s Battle with Software Giants Escalates, *Automotive News* (Dec. 26, 2016).



The price increase is therefore automatic, and is measured by the Customer Price Index plus 2%. The standard CDK contract gives dealers price protection for the first year of the DMS contract, but imposes a 6% automatic yearly price increase thereafter. As a result, dealers are hit from both sides: rapidly escalating data integration fees and contractually mandated, annual DMS price hikes.

**B. Defendants' Anticompetitive Conduct Has Harmed Competition in Many Other Ways**

226. Besides the massive, supracompetitive price increases for data integration services, Defendants have harmed competition in many other ways as well.

227. First, Defendants' conduct reduces dealership and vendor choice in the data integration market. Many dealerships and vendors prefer using Authenticom because of its superior product and service (and cheaper price), but Defendants are preventing dealerships and vendors from making that choice. Defendants require dealers and vendors – i.e., the customers on both sides of the Dealer Data Integration Market – to use Defendants' integration services regardless of the customers' preferences. And dealers and vendors have no choice given the elimination of competitors, the blocking of Authenticom, and the exclusive dealing provisions.

228. Second, Defendants' conduct is also reducing output in the data integration market, as well as the downstream market for third-party applications. Dealers are on record stating that they do not use some of their preferred vendors because of the huge pass-through data integration fees. Instead, the dealers either go without a vendor for that particular service, or they use a less preferable alternative (usually the one offered by CDK and Reynolds). There has also been reduced output in terms of fewer overall connections. And because Defendants now charge some vendors an additional per-transaction fee, those vendors are economizing by reducing the output of data they receive.

229. Third, Defendants' actions are thwarting innovation and reducing product quality in the third-party application market. The market for third party applications exploded due to the reliable and inexpensive access to dealer data provided by Authenticom and other independent data integrators. But now, dramatically more expensive data access means fewer new vendors and less opportunity for vendors to innovate. Moreover, many vendors have made the hard realization that their businesses are no longer sustainable with the higher data access costs and have exited the market. Dealers are therefore left with fewer products and services from which to choose. Even though vendors generally pass on a substantial percentage of the increased data costs to dealers, many vendors have no choice but to absorb some of the increased data fees – resulting in slashed budgets for research and development, support, and other investments in their products. These cost-cutting measures will ultimately reduce the quality of the products and diminish the support that the dealers receive.

230. Fourth, Defendants' actions have reduced the quality of data integration itself. By propping up their inferior data integration products, and trying to eliminate a superior one (Authenticom's DealerVault product, for example, with its dealer control and visibility over data extraction and syndication), Defendants are reducing the quality of the products in the market. As one Mercedes dealership in California wrote, "I am as sick of [CDK] . . . trying to force us into using their inferior offerings."

231. Finally, in concentrated markets, injury to a competitor harms not just that competitor, but competition generally. CDK and Reynolds have already driven out all of their competitors except for one – Authenticom. By driving Authenticom out of business, Defendants are by definition harming competition in the concentrated (indeed, monopolized) CDK and Reynolds Dealer Data Integration aftermarkets.

**V. Authenticom Has Suffered Antitrust Injury**

232. The same anticompetitive conduct that has injured competition has also directly and significantly damaged Authenticom. Defendants' written market division agreement caused many vendors to leave Authenticom for Digital Motorworks (i.e., CDK) during the "wind-down period" because those vendors knew they would not be blocked during that period, even if the vendors eventually would be forced to join the RCI program. The written agreement also was a key component of Defendants' overarching agreement to eliminate competition – including Authenticom – in the primary data integration market and the secondary aftermarkets. Defendants' exclusive dealing provisions prohibit dealers and vendors from using Authenticom's data integration services. And in carrying out their campaign to drive out competitors, Defendants have continuously disrupted Authenticom's ability to access dealer data by, among other tactics, disabling Authenticom's dealer-created log-in credentials.

233. Because Authenticom's business and revenues depend on its ability to access dealer data and provide data integration services to dealers and vendors, Defendants' anticompetitive conduct has nearly destroyed the entirety of Authenticom's business. As a result of Defendants' actions, the number of data feeds that Authenticom has established for vendors has sharply declined. Authenticom's profits, as measured by EBITDA, dropped by 77.22 percent from the third quarter of 2015, when Defendants intensified their blocking efforts, to the first quarter of 2017. Defendants' actions have left Authenticom cash flow insolvent, with insufficient earnings and resources to satisfy its outstanding debt obligations. Authenticom was unable to pay an \$11 million principal payment on a loan from BMO Harris Bank due April 16, 2017, and has received a limited 90-day forbearance from the Bank pending the outcome of the forthcoming preliminary injunction motion. Authenticom was also unable to pay an approximately \$1.17 million tax-related obligation due April 18, 2017. Authenticom has sought

additional financing from, among others, BMO Harris Bank and Citizens State Bank, but they have declined to provide this financing, citing doubts about Authenticom's continued viability because of Defendants' actions.

#### **VI. Defendants' Anticompetitive Conduct Has No Pro-Competitive Justification**

234. There are no pro-competitive justifications that excuse Defendants' misconduct. Defendants' conduct has not reduced price, increased output, or improved quality. On the contrary, as outlined above, Defendants' anticompetitive conduct has dramatically increased prices, reduced output, restricted customer choice, suppressed innovation, and diminished product quality.

235. Defendants' argument for their anticompetitive conduct is that it is necessary to protect "data security." By extension, Defendants have claimed that Authenticom (and all other independent data integrators) are "unsecure" and pose a threat to the security of dealer data. In other words, CDK and Reynolds argue that, in order to protect dealer data, it is necessary for them to (1) agree to divide the data integration market; (2) impose exclusive dealing provisions in vendor and dealer contracts; (3) agree to block independent data integrators from pulling data; and (4) drive out all competitors from the data integration market, including Authenticom. Instead of protecting dealer data, the only fruits of that anticompetitive conduct are monopoly profits and the protection of Defendants' DMS duopoly.

236. As evidenced by many facts, Defendants' "security" rationale is a pretext.

237. First, there is nothing unusual or unsecure about independent data integrators like Authenticom. CDK owns two data integrators – Digital Motorworks and IntegraLink – that pull and syndicate data in the same way as Authenticom: using login credentials provided by the dealer and then transferring the data to vendors. Malcolm Thorne – CDK's then chief strategy officer – told *Automotive News* in March 2015 that "the pull process of extracting data is as safe

as pushing out.” Indeed, until they entered their agreement in February 2015, CDK pulled data using login credentials from Reynolds dealers, and CDK continues to pull data in this way from dealers using other DMS systems. And Reynolds for over a decade allowed independent data integrators to provide services for Reynolds dealers. It was only after Mr. Brockman acquired the company that it changed positions. A top-level CDK executive admitted in private conversation with a vendor that the rhetoric around “security” has “little credibility” and is primarily designed to force vendors to use CDK for data integration.

238. Using login credentials to pull data is standard across industries, including in banking and healthcare, where the data is much more sensitive than anything accessible from dealers. Taking the banking industry as an example, thousands of third party applications – from well-established ones like PayPal, Mint, Square, and Quicken to new startups like Even – require access to a customer’s banking data. There are large data integrators like Intuit and Yodlee that pull data from the consumers’ bank accounts using login credentials and provide that data to the third party applications. As the Consumer Financial Protection Bureau recently summarized, “Typically, consumers provide their account credentials for a particular company or financial institution where they hold an account. Those credentials are then used to obtain their account data through either: (1) A structured data feed or an application program interface (API) hosted by the company or financial institution, or (2) the company or financial institution’s consumer-facing website in a process known as screen-scraping.”<sup>38</sup> Indeed, “screen scraping is the only technology that enables all of the thousands of small financial institutions to participate in the data-sharing ecosystem.”<sup>39</sup> And that ecosystem – just as in the automobile industry – has been

---

<sup>38</sup> *Consumer Access to Financial Records*, Request for Information, Bureau of Consumer Financial Protection, Docket No.: CFPB-2016-0048, at 9 (Nov. 17, 2016).

critical for the development of many innovations in the banking industry. As the Consumer Financial Protection Bureau stated, “the availability of consumer financial account data . . . has made possible a range of benefits to consumers.”<sup>40</sup>

239. Mr. Brockman has justified Reynolds’ blocking of independent data integrators by arguing that there is “within the dealership system as much personal information as there would be inside banks. Can you imagine a bank that would have a dial-in modem attached to its system where, if the bank felt like it, it could give out the password and let third parties access it? The suggestion is ludicrous.”<sup>41</sup> In fact, contrary to Mr. Brockman’s suggestion, that is exactly what happens in the banking industry. Mr. Brockman got his analogy wrong in another way: it is the actual customer, the owner of the data, that provides the login credentials, not the bank or the DMS provider.

240. Second, as a substantive matter, CDK and Reynolds have no basis to claim that Authenticom is unsecure. Authenticom has never had a data breach and its firewall has never been compromised. Authenticom pulls data using standard industry protocols. To transfer data, Authenticom uses encryption protocols that meet or exceed federal standards for banking transactions. Microsoft has certified Authenticom with its top-level gold security certification three years in a row. If there was a security incident (and there never has been one), Authenticom has agreed to indemnify dealers for any resulting harm. Authenticom is also insured with a \$20 million dollar cyber liability insurance policy. Authenticom has an information security system that is in full accordance with applicable consumer privacy and

---

<sup>39</sup> Jennifer Tescher and Beth Brockland, *One-off Data-Sharing Deals Aren’t Enough*, American Banker (Jan. 27, 2017).

<sup>40</sup> *Consumer Access to Financial Records*, Request for Information, Bureau of Consumer Financial Protection, Docket No.: CFPB-2016-0048, at 7 (Nov. 17, 2016).

<sup>41</sup> Ralph Kisiel, *Question & Answer: Deal Puts Brockman in the Spotlight*, Automotive News (Feb. 19, 2007).

protection restrictions, including the Gramm-Leach-Bliley Act of 1999 and the Federal Trade Commission's Implementing Rules. Indeed, dealers require that Authenticom comply with data privacy regulatory requirements. In short, CDK and Reynolds have no basis to use "data security" as a reason to destroy Authenticom's business.

241. Third, as detailed above, Reynolds and CDK actually use Authenticom as a data integrator for certain of their third party applications. CDK and Reynolds pay Authenticom to pull data from dealerships using their DMS systems and distribute that data to their applications. Furthermore, one Defendant has agreed to stop disabling Authenticom's login credentials for one of the Defendant's largest dealer customers in response to that dealer's demands. Only a select few dealership groups has this customer's size and clout. But the fact that Authenticom pulls data from this large dealership group with the Defendant's blessing – in addition to the fact that Reynolds and CDK actually use Authenticom for integration services – proves there is nothing "unsecure" about Authenticom's process or security protocol.<sup>42</sup>

**FIRST CAUSE OF ACTION:**  
**HORIZONTAL CONSPIRACY IN VIOLATION OF**  
**SECTION 1 OF THE SHERMAN ACT**

242. Authenticom incorporates by reference the preceding allegations.

243. CDK and Reynolds entered into and engaged in an agreement in restraint of trade in violation of Section 1 of the Sherman Act, 15 U.S.C. § 1, and Section 4 of the Clayton Act, 15 U.S.C. § 15.

---

<sup>42</sup> If CDK and Reynolds were concerned about data security instead of monopoly profits, then there are a number of less restrictive means to protect dealer data. Most obviously, they could establish "application program interfaces" – called APIs – with independent data integrators. Before entering the agreement with Reynolds, CDK even advocated that DMS providers should establish APIs for data integrators. Indeed, some of the smaller DMS providers do provide APIs for Authenticom, Digital Motorworks, and IntegraLink. Other DMS providers send regularly scheduled data reports to Authenticom, which is another less restrictive means. There are many others. Moreover, Authenticom has repeatedly offered to discuss its security protocols with CDK and Reynolds. Not once have Defendants taken Authenticom up on its offer.

244. CDK and Reynolds are horizontal competitors of one another in the DMS Market and the Dealer Data Integration Market.

245. The conspiracy between CDK and Reynolds consists of a continuing agreement, understanding, or concerted action to eliminate competition in the Dealer Data Integration Market and their respective aftermarkets. In furtherance of that conspiracy, in February 2015, they entered into a written market division agreement pursuant to which they agreed to no longer compete in the Dealer Data Integration Market. CDK and Reynolds also engaged in a group boycott to block all other third-party data integrators (such as Authenticom) from accessing data of dealers using Defendants' respective DMS systems. Defendants' conspiracy is a per se violation of the federal antitrust laws and is, in any event, an unreasonable and unlawful restraint of trade and commerce.

246. The purpose of Defendants' conspiracy is twofold: (1) to protect their DMS duopoly and (2) to drive competing data integrators out of the Dealer Data Integration Market and their respective aftermarkets, thereby protecting and increasing the flow of monopoly profits to CDK and Reynolds.

247. Defendants' conspiracy was intended to harm interstate commerce, and it has had an actual, substantial effect on interstate commerce.

248. Through their conspiracy, Defendants have caused actual injury to competition in the Dealer Data Integration Market and their respective aftermarkets.

249. The CDK and Reynolds agreement has cut off Authenticom's access to dealer data that Authenticom needs in order to compete with CDK and Reynolds in the Dealer Data Integration Market.



250. CDK and Reynolds possess dominant positions in the DMS Market, which they have utilized to further the conspiracy.

251. Defendants' conspiracy and anticompetitive conduct in furtherance thereof do not enhance efficiency or competition in the Dealer Data Integration Market. On the contrary, Defendants' conduct has produced only anticompetitive effects in that market.

252. As a direct and proximate result of Defendants' unlawful conduct, Authenticom has suffered injury to its business or property. Authenticom is entitled to treble damages for the violations of the Sherman Act alleged herein.

**SECOND CAUSE OF ACTION:**  
**EXCLUSIVE DEALING PROVISIONS IN VIOLATION OF**  
**SECTION 1 OF THE SHERMAN ACT**

253. Authenticom incorporates by reference the preceding allegations.

254. CDK and Reynolds entered into contracts with dealers and vendors that contain exclusive dealing provisions that unreasonably restrain trade in violation of Section 1 of the Sherman Act, 15 U.S.C. § 1, and Section 4 of the Clayton Act, 15 U.S.C. § 15.

255. Pursuant to their conspiracy to eliminate competition in the Dealer Data Integration Market and respective aftermarkets, CDK and Reynolds inserted exclusive dealing provisions in their contracts with dealers and vendors. The contracts with dealers provide that dealers cannot provide access to their data to any data integrator except CDK or Reynolds, respectively. Likewise, the contracts with vendors provide that vendors cannot obtain data for dealers using the CDK or Reynolds DMS systems from any data integrator except CDK or Reynolds, respectively. These provisions are standard throughout Defendants' contracts with dealers and vendors.

256. CDK and Reynolds were able to impose these exclusive dealing provisions on dealers and vendors as a result of their market power in the DMS Market (dealers) and the Data Integration Market (vendors).

257. Because CDK and Reynolds imposed these exclusive dealing provisions pursuant to their conspiracy to eliminate competition in the Dealer Data Integration Market and respective aftermarkets, they are per se illegal. Nevertheless, whether entered into pursuant to an agreement between Defendants or independently, because these agreements, individually and collectively, unreasonably foreclose competition in a substantial portion of the Dealer Data Integration Market and are likely to, and in fact have, led to increased prices in that market beyond competitive levels, these agreements constitute an unreasonable and unlawful restraint of trade under the rule of reason.

258. Through these exclusive dealing provisions, Defendants have caused actual injury to competition in the Dealer Data Integration Market.

259. The exclusive dealing agreements have, individually and collectively, substantially foreclosed Authenticom's access to dealer data that Authenticom needs in order to compete with CDK and Reynolds in the Dealer Data Integration Market.

260. Defendants' exclusive dealing agreements do not enhance efficiency or competition in the Dealer Data Integration Market. On the contrary, the agreements have produced only anticompetitive effects in that market.

261. As a direct and proximate result of Defendants' unlawful conduct, Authenticom has suffered injury to its business or property. Authenticom is entitled to treble damages for the violations of the Sherman Act alleged herein.

**THIRD CAUSE OF ACTION:**  
**ILLEGAL TYING IN VIOLATION OF SECTION 1 OF THE SHERMAN ACT**

262. Authenticom incorporates by reference the preceding allegations.

263. CDK and Reynolds have imposed tying arrangements on dealers that unreasonably restrain trade in violation of Section 1 of the Sherman Act, 15 U.S.C. § 1, and Section 4 of the Clayton Act, 15 U.S.C. § 15.

264. CDK and Reynolds have tied dealers' use of Defendants' integration services to their DMS services. That is, as a condition of dealers using Defendants' DMS services, Defendants also require dealers to use Defendants' own integration services and not use their competitors' integration services. Thus, Defendants coerce customers of their DMS systems – i.e., the dealers – into using Defendants' dealer data integration services.

265. DMS systems are a separate and distinct product from dealer data integration services.

266. Defendants have sufficient market power in the tying market (the market for DMS services, where they have had a longstanding duopoly) to appreciably restrain free competition in the market for the tied product (dealer data integration services). Defendants have demonstrated their ability to leverage their market power in the tying market (DMS services) to control prices and exclude competition in the tied market (integration services).

267. Defendants' tying arrangements have affected a substantial amount of interstate commerce.

268. Defendants' tying arrangements are a per se violation of the federal antitrust laws and are, in any event, unreasonable and unlawful restraints of trade and commerce.

269. As a direct and proximate result of Defendants' unlawful tying arrangement, Authenticom has suffered injury to its business or property. Authenticom is entitled to treble damages for the violations of the Sherman Act alleged herein.

**FOURTH CAUSE OF ACTION:**  
**MONOPOLIZATION OF THE DEALER DATA INTEGRATION AFTERMARKETS IN**  
**VIOLATION OF SECTION 2 OF THE SHERMAN ACT**

270. Authenticom incorporates by reference the preceding allegations.

271. Defendants CDK and Reynolds have unlawfully monopolized their respective Dealer Data Integration aftermarkets in violation of Section 2 of the Sherman Act, 15 U.S.C. § 2.

272. In the primary DMS product market, Defendants have a longstanding duopoly. When dealers purchase Defendants' brand of DMS, they are "locked in" to that brand through long-term contractual relationship and high switching and information costs.

273. Because of customer lock-in in the primary DMS market, Defendants have monopolized the aftermarkets for dealer data integration services on their respective DMS platforms. CDK and Reynolds have demonstrated their ability to control prices and exclude competition by blocking third-party integrators from accessing dealer data stored on their systems and by profitably raising integration fees to supracompetitive levels.

274. CDK and Reynolds used anti-competitive means to acquire and maintain their monopolies in the aftermarkets for dealer data integration services, including, *inter alia*, by blocking and disabling third-party integrators from accessing dealer data, entering into a market division agreement pursuant to which they agreed not to compete in the aftermarkets, and imposing anticompetitive exclusive dealing arrangements on vendors and dealers.

275. Defendants' ability to exclude competition and impose massive price increases demonstrate their market power in the aftermarkets. And such conduct has no procompetitive business justification.

276. As a direct and proximate result of Defendants' unlawful conduct, Authenticom has suffered injury to its business or property. Authenticom is entitled to treble damages for the violations of the Sherman Act alleged herein.

**FIFTH CAUSE OF ACTION:**  
**TORTIOUS INTERFERENCE**

277. Authenticom incorporates by reference the preceding allegations.

278. Defendants have tortiously interfered with Authenticom's existing contracts with dealers and vendors, in violation of Wisconsin state law.

279. Authenticom has contracts with thousands of dealers. In those contracts, dealers contract with Authenticom to extract dealer data for purposes of providing data integration services. Authenticom also has contracts with hundreds of vendors. In those contracts, vendors contract with Authenticom to provide them with standardized dealer data for use in the vendors' applications.

280. Both CDK and Reynolds tortiously interfered with Authenticom's contracts with dealers and vendors when they blocked Authenticom from providing dealer data integration services, including by disabling Authenticom's dealer-created login credentials. CDK and Reynolds likewise interfered with Authenticom's dealer and vendor contracts by spreading false and disparaging information about Authenticom's security practices and protocol.

281. Both CDK and Reynolds knew about Authenticom's contracts with dealers and vendors when they interfered with those contracts. In fact, many of Authenticom's contracts with dealers and vendors predated any contract that Defendants may have with those third parties.

282. As a result of Defendants' interference, many dealers and vendors terminated their contracts with Authenticom. Defendants' interference was intentional and designed to produce this result.

283. Defendants' interference damaged Authenticom by causing its vendor and dealer customers to terminate their contracts with Authenticom, and leave Authenticom's data integration business and go to Defendants' integration businesses.

284. It was foreseeable to Defendants that their interference would cause these damages. In fact, Defendants specifically intended to cause these damages by blocking Authenticom and preventing it from being able to provide data integration services.

285. Defendants were not justified or privileged to interfere with Authenticom's contracts. Indeed, Defendants' interference was and is illegal under federal antitrust laws.

286. At trial, Authenticom will prove the precise amount of damages suffered.

### **JURY DEMAND**

In accordance with Federal Rule of Civil Procedure 38(b), Authenticom demands a trial by jury on all issues so triable.

### **PRAYER FOR RELIEF**

WHEREFORE, Authenticom requests that the Court:

(a) decree that the conduct alleged herein is an illegal restraint of trade in violation of Section 1 of the Sherman Act;

(b) decree that the conduct alleged herein is an illegal monopoly, attempted monopolization, and conspiracy to monopolize in violation of Section 2 of the Sherman Act;

(c) decree that the exclusive dealing provisions in Defendants' contracts with vendors and dealers are anticompetitive and illegal restraints of trade under Section 1 of the Sherman Act;

(d) preliminarily and permanently enjoin the enforcement of the exclusive dealing provisions in the CDK and Reynolds contracts with dealers and vendors;

(e) preliminarily and permanently release vendors from the term commitments (i.e., the multi-year terms) in their contracts with CDK and Reynolds;

(f) preliminarily and permanently enjoin CDK and Reynolds from blocking or disabling Authenticom's access to dealer data for purposes of providing dealer data integration services;

(g) award Authenticom damages, as provided under the Sherman Act, and that a joint and several judgment in favor of Authenticom be entered against Defendants in an amount to be trebled in accordance with such laws;

(h) award Authenticom its reasonable costs and expenses incurred in this action, including expert fees and attorney's fees;

(i) award Authenticom prejudgment interest; and

(j) award Authenticom any such further relief that the Court may deem just and proper.

May 1, 2017

Respectfully submitted,

/s/ Jennifer L. Gregor

Jennifer L. Gregor  
Mark W. Hancock  
GODFREY KAHN S.C.  
One East Main Street  
Suite 500  
Madison, Wisconsin 53703  
Telephone: (608) 284-2629  
Fax: (608) 257-0609  
jgregor@gklaw.com  
mhancock@gklaw.com

Michael N. Nemelka  
Aaron M. Panner  
Derek T. Ho  
Joshua Hafenbrack  
Joanna T. Zhang  
Benjamin L. Rudofsky  
KELLOGG, HANSEN, TODD,  
FIGEL & FREDERICK, P.L.L.C.  
1615 M Street, N.W., Suite 400  
Washington, D.C. 20036  
Telephone: (202) 326-7900  
Fax: (202) 326-7999  
mnemelka@kellogghansen.com  
apanner@kellogghansen.com  
dho@kellogghansen.com  
jhafenbrack@kellogghansen.com  
jzhang@kellogghansen.com  
brudofsky@kellogghansen.com

*Counsel for Plaintiff Authenticom, Inc.*