UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MICHIGAN
NORTHERN DIVISION

DICE CORPORATION,

Plaintiff,

v.

Case Number 11-13578
Honorable Thomas L. Ludington

BOLD TECHNOLOGIES,

Defendant.
_____/

OPINION AND ORDER GRANTING DEFENDANT'S MOTION FOR SUMMARY JUDGMENT AND DISMISSING COMPLAINT WITH PREJUDICE

In this intellectual property dispute, Plaintiff Dice Corporation alleges that Defendant Bold Technology accessed Plaintiff's servers and stole its software. Defendant denies that it did any such thing. Relying on deposition testimony, affidavits, and other evidence showing that it neither accessed Plaintiff's servers nor its software, Defendant now moves for summary judgment. Plaintiff opposes the motion. The opposition, however, is based on conclusory assertions, not evidence. The Court will grant Defendant's motion.

I

A

Plaintiff is a Michigan corporation with its principal place of business in Bay City, Michigan. Second Am. Compl. ¶ 1. It was founded in 1992 by Mr. Clifford Dice, who is its president, chief executive officer, and sole owner. Dice Dep. 7, Feb. 29, 2012, *attached as* Def.'s Mot. for Summ. J. Ex. A. Defendant is an Illinois corporation with its principal place of business in Colorado Springs, Colorado. *Id.* ¶ 2.

Competitors, Plaintiff and Defendant both provide software for companies in the alarm industry. Dice Dep. 8, 13; Coles Aff. ¶ 3, *attached as* Def.'s Mot. Ex. B. That is, Plaintiff and Defendant license software enabling alarm companies to monitor their customers' alarms. Customers pay the alarm companies to monitor various types of alarms (such as burglar and fire alarms). Coles Aff. ¶ 3; *see* Dice Aff. ¶ 4, *attached as* Pl.'s Resp. to Def.'s Mot. for Summ. J. Ex. A. The alarms send signals to receivers located at the alarm companies. Coles Aff. ¶ 3. When an emergency signal is sent, the company contacts the appropriate authorities (such as police or fire departments). *Id*. Larger alarm companies have hundreds of thousands of customers. *Id*. ¶ 4. Companies like Plaintiff and Defendant create the software that monitors the signals. *Id*.

To operate their businesses, the alarm companies must also collect large amounts of data regarding their customers, including "names, addresses, contact information, billing information, [and] information regarding the type and location of alarms." *Id*. The data is compiled in databases within software that the alarm companies license from companies like Plaintiff and Defendant. *Id*.

On a basic level, Plaintiff's and Defendant's software thus performs the same functions: compiling information and monitoring signals for the alarm companies. Coles Aff. ¶ 3. On a technical level, however, the software is much different. Plaintiff's software operates on a Linux platform and is written in the Thoroughbred Basic computer language.[1] Narowski Aff. ¶ 5, *attached as* Def.'s Mot. Ex. D. Defendant's software operates on a Windows platform and is written in the Microsoft computer languages C++ and Visual Basic. *Id*. Plaintiff licenses its

[1] *See generally Universal City Studios, Inc. v. Reimerdes*, 111 F. Supp. 2d 294, 305 (S.D.N.Y. 2000) (discussing operating systems and computer languages), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

software simply as "Dice software"; Defendant licenses its software under the trade name "Manitou." Coles Aff. ¶¶ 2–3.

B

One such alarm company, ESC Central, was one of Plaintiff's customers for a decade; it is now one of Defendant's customers. *See* Jennings (formerly Harris) Dep. 13, *attached as* Def.'s Mot. Ex. F. The present litigation arises out of this transition.

ESC Central provides services to about 400 dealers and 50,000 customers. Jennings Dep. 7. Located in Birmingham, Alabama, it began licensing Dice software in 2001. *Id*. at 6, 10.

ESC Central's operations manager is Kristi Jennings (formerly Harris). During the decade that ESC Central was one of Plaintiff's customers, Ms. Jennings was actively involved in Plaintiff's operations, chairing its "user group," serving on its "chart committee," and even selling software on Plaintiff's behalf.

The "user group" received suggested software changes to Plaintiff's software from customers. *Id*. at 12. The group would then meet and vote on which features to incorporate into future editions of Plaintiff's software. *Id*. Ms. Jennings chaired Plaintiff's user group from 2005 through 2010. *Id*. at 11.

Ms. Jennings was also a member of Plaintiff's "chart code committee." *Id*. at 20. The alarms are programed to send signals to receivers located at the alarm companies' offices. Signals include alerts for fire, flood, burglary, and other types of events. The "event codes," however, vary from manufacturer (for example, one manufacture would code fire as "1" while another would code fire as "3"). *Id*.

Plaintiff's chart code committee compiled this manufacturer information to update Plaintiff's "ALSCHART" file. *Id*. This file, Plaintiff's user manual explains, is a data file

containing information regarding "incoming signals from zones and other information about processing." *Dice Knowledge Base Article 3-1.2* (Sept. 12, 2003), *attached as* Def.'s Mot. Ex. G. Discussing the chart committee's responsibility, Ms. Jennings explained in her deposition: "Our task was to chart codes from manufacturers and submit them to Dice." Jennings Dep. 20. She was then asked:

> Q: So how would you go about doing that?
> A: We would contact the manufacturers and ask them . . . .
> Q: So what did Dice do with the chart codes that were submitted by the committee?
> A: They would take it and update it inside Dice software.
> Q: And where in the Dice software would we go to find this listing of all the codes?
> A: Within their chart codes.
> Q: Where is that? What is the name of that file?
> A: The ALS[CHART] codes.
> Q: ALS[CHART]?
> A: Yes. . . .
> Q: And just to be clear, they were — these codes were simply the manufacturers' codes that had been assigned by the various manufacturers for these various types of signals, and then these codes were all accumulated within this file called ALS[CHART] which was part of the Dice software?
> A: Yes.

Jennings Dep. 20–22. *See also Dice Knowledge Base Article* (Sept. 12, 2003). And Ms. Jennings also sold software on Plaintiff's behalf. *Id*. at 13. In her deposition, she was asked:

> Q: Well, to be able to do that, did you have any particular training or knowledge on the software that would allow you to effectively sell the software for Dice?
> A: The best sales tool to me is the fact that I used it every day, and I knew the in's and out's of the software and how it worked.
> Q: Would you consider yourself to be extremely knowledgeable on the Dice software?
> A: Yes.
> Q: So how many times do you think you actually did sales demos for Dice?
> A: I don't know an exact number. If I was to estimate, I would say at least 20 times.

Jennings Dep. 13–14.

C

Before the Dice user group meeting in August 2010, Ms. Jennings emailed Plaintiff with concerns. Def.'s Mot. Ex. H. "I'm going to tell you that this may be a make or break year for [the Dice user group]," Ms. Jennings wrote, elaborating: "There are several companies not coming because 'Dice is going to do what they want not what the users want' and 'it's just a waste of time and money.' . . . I am not going to sugar coat all the things that I have heard and I don't want a call telling me how great things are or how many systems are being sold. There are a number of unhappy customers." *Id*. at 2.

Plaintiff's founder and CEO, Mr. Dice, responded via email: "[W]e are not trying to sell anything. We have to [pare] down the number of clients we have and serve due to the larger scale of the product line currently. Once folks see what our direction is and what our development cycles are[,] [i]f they are not pleased with our direction, they should contact the competition and move quickly to another [software provider] as you indicated, [and] I would encourage it." *Id*.

In September 2010, Ms. Jennings again emailed Plaintiff with concerns. Def.'s Mot. Ex. I. Noting that the software had crashed ESC Central's phone system, Ms. Jennings wrote: "We are aware that DICE seems to think that the Altigen flakiness might be fixed by upgrading. However, before doing anything else with this stupid phone system I want assurances in writing from someone at DICE that this will stop these issues." *Id*. at 2.

Mr. Dice responded: "On one hand, I feel responsible for not configuring multiple boxes, but after kicking myself over and over again[,] I am not sure how I would have known that I needed to. Given the fact that you were a beta site, we all know that the expectation is, that we will all learn things and may change the situation. To make things worse, the relationship

between you and I has not been good, and getting worse." *Id*. at 1. He concluded: "So I am sorry that you have had the bad experience. And I want you to know that I want to fix it, but you have to trust us and we have to work closely again. Otherwise, I think it's just better if you start backing out of what you have and planning longer term a change to some other automation system." *Id*. at 2; *but see* Dice Aff. ¶ 9 ("ESC was not asked to terminate its relationship with Dice and did not leave Dice because of quality issues.").

D

In October 2010, Ms. Jennings took up Mr. Dice on his suggestion that she should contact the competition if she was dissatisfied and emailed Defendant. Jennings Dep. 32–33. In Ms. Jennings' deposition, she was asked:

> Q: [Was] this the first contact that you had in terms of moving from Dice over to Bold?
> A: Yes.
> Q: At this point in time in October 2010, I mean, had you absolutely made up your mind you were leaving or you were just looking around?
> A: No, I just started looking.
> Q: Did you look at other Dice competitors beside Bold?
> A: Yes.

Id. Also in October 2010, Mr. Dice disbanded the users group. Id. at 22.

In February 2011, Ms. Jennings reached what she "called my final straw." Jennings Dep. 36. Finding ESC Central's system was crashing each night, she wrote to Defendant: "I am being blasted by complaints from operators, dealers, and anyone else that is having to deal with this system. I can pretty much guarantee that if we call with a problem it involves some aspect of the phone system not working properly. . . . We now have more points of failure than was ever imaginable before! We haven't heard a solution other than reboot it and see if it works better." Def.'s Mot. Ex. J.

Dissatisfied with Plaintiff's response to this problem, in April 2011 ESC Central signed a software licensing agreement with Defendant. Jennings Dep. 38; *but see* Dice Aff. ¶ 9 (asserting ESC Central "did not leave Dice because of quality issues").

E

Defendant then began converting ESC Central from Plaintiff's software system to Defendant's system. "Generally speaking," Defendant's chief of operations explains, "the process of converting a customer from one software system to another must be done carefully. Because the customer is actively monitoring alarm signals from thousands of subscribers, the transition from one software to another must be done seamlessly." Coles Aff. ¶ 5. He notes that the transition can take several months, elaborating:

> After the customer signs a license agreement for the new software, one of the first steps in the conversion process is the conversion of the customer's data regarding their subscribers from databases in the old software to databases in the new software. After the customer data is extracted and converted, there will be a period of time, usually about three months, when a customer's central station is running live on the old software, but the new software is running in parallel on different servers. The purpose of running the two software systems in parallel is to ensure that the new software is monitoring the alarm signals consistent with the old software. After this period is completed the customer will go live on the new software and will often terminate its license for the old software.

Id. ¶ 6; *see also* Dice Dep. 72 (noting that Plaintiff moves customers onto its system by having the two systems run parallel for a time).

To transition ESC Central from Plaintiff's system to Defendant's system without interrupting customer operations, Defendant first extracted ESC Central customer data from Plaintiff's software databases. *See* Coles Aff. ¶ 6 (quoted above); Narowski Aff. ¶ 4. Specifically, Defendant extracted ESC Central's customer "names, addresses, contact information, billing information, information regarding the type and location of alarms." Coles

Aff. 4; *see* Dice Dep. 24, 147 (acknowledging that this information is owned by the customer, not Plaintiff).

Matt Narowski, a computer programmer employed by Defendant, wrote the program to extract this data from Plaintiff's software (written in Thoroughbred basic) and convert it into a format that can be read by Defendant's software (written in C++ and Visual Basic). Narowski Aff. ¶¶ 4–7. He explains:

> The function of the Extraction Program is to extract the customer data from databases stored on the Linux operating platform used by Dice software. The customer data is extracted in a comma-separated text file, which is a format that Bold uses to convert the customer data into Manitou, which is the trade name of Bold software. It is my understanding that the extraction program is run after the customer has decided to replace its Dice software with Bold's software and the customer wants to extract its data from the databases where it is stored. There are several other programs available which could extract the customer data from the databases, such as Thoroughbred Query, which is a Thoroughbred product, and products available through Linux. The Extraction Program that I wrote differs from these methods because it converts the customer data into the comma-separated text file format which is more easily utilized for conversion into Bold's Manitou software.
>
> The Extraction Program is not capable of operating an alarm company central station or of monitoring or processing an alarm signal, which is my general understanding of the function of the Dice software.

Id. ¶¶ 7–8. Discussing how he created the program, Mr. Narowski continues:

> I wrote the Extraction Program using information available to the public regarding Thoroughbred Basic together with my general knowledge of computer programming. I did not read, review, copy, or rely upon any information about Dice source code or Dice object code when I wrote the Extraction Program, and the Extraction Program does not contain any Dice source code or object code. In fact, since I have been employed at Bold I have not seen a copy of Dice source code or Dice object code.

Id. ¶ 6.[2] He emphasizes:

[2] For those unfamiliar with computer programing, Judge Kaplan explains:

> Computers come down to one basic premise: They operate with a series of on and off switches, using two digits in the binary (base 2) number system—0 (for off) and 1 (for on). All data and instructions input to or contained in computers therefore must be reduced to . . . 1 and 0. . . .

> The Extraction Program does not read or copy any source code, object code or signal processing software of Dice and is not capable of doing so.
>
> The Extraction Program does not circumvent any security feature built into the Dice software. Dice has security features built into portions of its software which prevent unauthorized users from running those protected portions of the software. However, the database files where the customer data is stored are not subject to any Dice security features and can be accessed by anyone who has a copy of Thoroughbred basic, which Bold licensed from that company.

Id. ¶¶ 9–10. Mr. Dice acknowledged in his deposition that Plaintiff has offered no evidence, at least no evidence that is admissible,[3] that Defendant has copied Plaintiff's source code. He was asked:

> Q: Are you claiming that Bold has actually copied Dice's source code?
> A: To some extent, yes.
> Q: What source code are you claiming they copied?
> A: The copywritten materials.
> Q: And what is your proof that they copied your source code?
> A: At this point the only proof we have is that they've been converting our customers using our data that was supplied with the system because they took it . . . .
> Q: So you've never looked at Bold's code; is that right?
> A: Absolutely not.
> Q: So you don't know for a fact that Bold copied Dice's source code, right?
> A: No, we don't know that for a fact.

> Some highly skilled human beings can reduce data and instructions to strings of 1's and 0's and thus program computers to perform complex tasks by inputting commands and data in that form. But it would be inconvenient, inefficient and, for most people, probably impossible to do so. In consequence, computer science has developed programming languages. These languages, like other written languages, employ symbols and syntax to convey meaning. The text of programs written in these languages is referred to as source code. And whether directly or through the medium of another program, the sets of instructions written in programming languages — the source code — ultimately are translated into machine "readable" strings of 1's and 0's, known in the computer world as object code, which typically are executable by the computer.

Universal City Studios, Inc. v. Reimerdes, 111 F. Supp. 2d 294, 306 (S.D.N.Y. 2000) (quotation marks, footnotes, and internal alterations omitted), *aff'd sub nom. Universal City Studios, Inc. v. Corley*, 273 F.3d 429 (2d Cir. 2001).

[3] In Mr. Dice's deposition, he also references hearsay assertions made by third parties. *See, e.g*., Dice Dep. 166–68, 172–73.

Dice Dep. 166–67; *see id*. at 61 (acknowledging that Plaintiff's assertion that Defendant copied Plaintiff's source code is "an assumption"); *but see* Dice Aff. ¶ 6 ("The program which Bold has created for converting information belonging to Dice customers cannot operate without access to Dice software and the source code contained within that software"). Questioned further, Mr. Dice again acknowledged that he did not know if Defendant used Plaintiff's code:

> Q: [D]o you have any evidence that Bold is using the identical codes that Dice is using?
> A: Not until we go through all of their software and drivers.
> Q: So the answer to that question would be no, you don't?
> A: No, not at this point.

Dice Dep. 173.

Mr. Dice also acknowledged that ESC Central could access database files where customer data is stored and retrieve the data without circumventing any of Plaintiff's security measures. Dice Dep. 159. Third-party applications such as Thoroughbred Query allow users to type in commands, or "queries," to retrieve the data. In Mr. Dice's deposition, he was asked:

> Q: So no administrative password would have been used —
> A: No.
> Q: — for all these queries?
> A: It just required knowledge.

Dice Dep. 159. And Mr. Dice acknowledged that Plaintiff's software is not encrypted. In his deposition, he was asked:

> Q: [D]oes Dice . . . encrypt its software?
> A: We don't have the capacity to encrypt at an object code level. We can encrypt a source code, but we've had problems with it in the past so we tend not to encrypt anything.

Dice Dep. 28; *see id*. at 81 (acknowledging "We don't have a way of encrypting files").

E

In Mr. Narowski's deposition, he was also asked about another alarm company, Sonitrol, that has transferred its business from Plaintiff to Defendant. *See* Narowski Dep. 49–50, May 23, 2012, *attached as* Pl.'s Resp. Ex. C. Counsel asked:

> Q: And do you recall what form that data [conversion] took in Sonitrol matter?
> A: I don't recall. . . .
> Q: Showing you what has been marked as Exhibit 22, which is Bold document 3334.
> A: Huh. I did not re-collect — or recollect, sorry.
> Q: Is this another way to obtain information?
> A: It appears that they sent us an external hard drive with data on it. . . .
> Q: This Dice data would have included Dice programs?
> A: I can't recollect, but I would assume.
> Q: Dice data would include Dice drivers?
> A: That, I don't know.
> Q: But whatever was on this hard drive?
> A: We would have copied off.

Id. Mr. Narowski later elaborated:

> The "Dice Data" that I was referring to was data that was owned by [the client] regarding its subscribers that was stored in the databases that were on the hard drive I received for the purpose of converting the customer data from Dice software into Bold. . . . I do not know exactly what was included on the hard drive that [the customer] sent me. My concern was that the hard drive contain all of the customer data that [the client] needed converted. . . .
>
> As I explained in my original affidavit, the Bold extraction program does not circumvent any security features built into Dice software as it access databases in the Dice software . . . . During the conversion process Bold does not utilize any source code nor does it run any of the Dice software programs, such as the Dice receiver driver programs. Bold has never used Dice software for the purpose of monitoring alarm signals.

Narrowski Supp. Aff. ¶¶ 3, 7, *attached as* Def.'s Reply in Supp. Mot. for Summ. J. Ex. Z.

F

On May 27, 2011, Amy Condon left Plaintiff's employment and joined Defendant's firm. Second Am. Compl. ¶ 11. Over the next two weeks, Plaintiff's second amended complaint

alleges, "Ms. Condon accessed Dice servers located in Dice's Bay City facility and accessed file layouts that contained proprietary signal processing intelligence software." *Id*. ¶ 12. Ms. Condon flatly denies this. "Since I terminated my employment at Dice," her affidavit provides, "I have never accessed or attempted to access any server owned by Dice at its Bay City office or any other location." Condon Aff. ¶ 6, *attached as* Def.'s Mot. Ex. C.

Mr. Dice acknowledges that Plaintiff has no evidence that Ms. Condon accessed Dice servers. In his deposition, he was asked:

> Q: Are you claiming that Amy Condon hacked into the Dice servers in Bay City Michigan, yes or no?
> A: I don't think she hacked into anything. I don't — I don't know if she did or not. . . .
> Q: Did any Bold employees hack into Dice servers located in Bay City, Michigan?
> A: I don't know how Bold got our — got all of our intelligence. . . . It's not a question for me to answer, it's a question for you to answer. How did Bold get access to those files[?] . . .
> Q: So the answer to the question that I asked you is you don't know if some Bold employees hacked into the Dice servers located in Bay City, Michigan?
> A: I don't know how Bold got the information to be able to do what they've done. I have no idea. All I know is that they have it. . . .
> Q: Okay. I want to know [about] is this sentence [in paragraph twelve of the complaint] claiming that after Ms. Condon left her employment at Dice she somehow hacked into Dice's Bay City servers?
> A: That's what that says . . . .
> Q: All right. So on what dates did Miss Condon hack into the servers located in Dice's Bay City facility; what dates did that happen?
> A: We don't know.
> Q: Okay. How did she hack into the system?
> A: We don't know. . . .
> Q: And what are those things that you say prove that Ms. Condon hacked into the system, what are those things?
> A: You can see the query commands and what data she's accessing, which is our data, not client data.

Dice Dep. 35–41. Probing into this assertion later in the deposition, counsel asked Mr. Dice:

> Q: And what is the actual query command?
> A: It's basically — let's see. This one is of — our proprietary file that contains our data, ALSCHART.

Q: ALSCHART?
A: Yeah. It's the file that we provide with our software, and —
Q: So is the — is the customer allowed to access the ALSCHART [file]?
A: No.

Dice Dep. 129.

Notwithstanding Mr. Dice's assertion, Plaintiff's own director of software development, Julie Coppens, acknowledges that customers were allowed to access the ALSCHART file. Coppens Dep. 19, *attached as* Def.'s Mot. Ex. O.

In her deposition, Ms. Coppens first explained that she was the person who had first discovered that the queries at issue in this case had been run, testifying that in August 2011

I logged into Dice and checked some files and then I went to see what queries were ran.
Q: Okay. And what did you find?
A: It appeared that queries were ran in July that could have been used to convert off of Dice.
Q: To convert what?
A: Data off Dice.
Q: You mean the customer data?
A: Yes.
Q: Now the data that we are talking about, that belongs to the customer, right?
A: Specific data belongs to the customer.
Q: Just the data we're talking about that you are talking about being converted, right?
A: Yes.
Q: So these queries led you to believe that ESC wanted to take its data off of the Dice software and move it to a different software, right?
A: Uh-huh.
Q: Is that a yes?
A: Yes.
Q: That's what you suspected was going on?
A: Yes.
Q: Does the customer have the right to do that?
A: Yes.

Coppens Dep. 29.

G

Ms. Coppens further acknowledged that customers were specifically permitted access to the ALSCHART. Initially taking a contrary position in her deposition, Ms. Coppens first asserted that customers were prohibited from accessing the ALSCHART file. Coppens Dep. 18–19. On further questioning, however, Ms. Coppens revised her response:

> Q: Has it always been the case that Dice hasn't allowed access to the customers to see the chart table?
> A: Yes.
> Q: What's the chart table called, what's the code name for it?
> A: ALSCHART.
> Q: So if you put into Query select start ALSCHART with just a user's normal login, what would come up?
> A: Well, you can't use it in Query . . . .
> Q: So you can't access it through Query, this ALSCHART file?
> A: You cannot see the tables. You have to know — you have to know the specific field names in the table.
> Q: Give me an example. What's a specific field name in the table?
> A: When — say I had a database with customer field, let's say I had customer name, address, what type of panel that they were using, I can actually do a lookup on that file and see those field names in there. . . .
> Q: Why allow Query to access it though?
> A: To access what?
> Q: The ALSCHART table.
> A: We — previously we allowed the ability to create a table but you can't query the table anymore.
> Q: Wait a minute. You said previously you allowed the ability to query the table?
> A: Uh-huh.
> Q: When was that?
> A: Before September. You have to have knowledge of what to query.
> Q: So before September of 2011 —
> A: Uh-huh.
> Q: — okay, you were able to query the chart table, the ALSCHART table?
> A: Right.
> Q: So what changed in September of 2011?
> A: We found that you could query it.
> Q: So what you are telling me about today you can't query the ALSCHART table[,] that wasn't true a year ago, right?
> A: Right. A year ago you could type in the ALSCHART and the field names if you knew the field names.
> Q: And it would all come up?

A: Absolutely.
Q: It was not protected from the user, right? If you had the user login you could gain complete access to the [ALSCHART] — ALSCHART table a year ago, right?
A: Yes.

Coppens Dep. 19, 22–23; *but see* Dice Aff. ¶ 8 ("Bold also misleads this Court when it indicates that the information which Dice claims was misappropriated by Bold was readily available to Dice customers. Although Dice (or former Dice) personnel could access such proprietary information, this information was hidden from customers themselves.").

H

Ms. Coppens also confirms that an administrative password was not required to run the queries and that Plaintiff has no evidence of unauthorized access. Coppens Dep. 32, 77. She was asked:

Q: Is there any evidence that . . . Miss Condon after she left her employment at Dice or anyone else on Bold's behalf . . . somehow gain[ed] unauthorized access to Dice's software?
A: No one changed the code generator, if that's what you are asking.
Q: I'm — I'm asking you do you have any information or evidence that either Amy Condon or someone else at Bold Technologies somehow circumvented the Dice code generator protection on its software at any time?
A: Not to my knowledge.
Q: At any of [Plaintiff's] meetings or director meetings did anyone else indicate to you that they had learned that either Miss Condon or someone else on behalf of Bold had done something to circumvent this Dice code generator protection?
A: No.

Coppens Dep. 77–78.

Plaintiff's chief technical officer, the person directly responsible "for maintaining the security of the Dice servers in Bay City," confirms that Plaintiff has no evidence that any of Defendant's employees accessed Plaintiff's servers. Grecko Dep. 12, 21, 25, Mar. 1, 2012, *attached as* Def.'s Mot. Ex. Q. In his deposition, the gentleman was asked:

Q: Are you aware of any evidence, do you have any fact that you could point to to say that [Ms. Condon] actually accessed the Dice servers in Bay City, Michigan after she left the company?
A: No, there's no proof I can give you saying here's a document to say Amy did X, Y, Z.
Q: And there's no record or any — anything that would indicate that Amy made some type of unauthorized access the Dice system after she left her employment?
A: Well, as I explained earlier to you, that there's no way for me to tell. . . .
Q: So if Amy were to deny that she ever did that, that she ever accessed the Dice server [after] she left her employment, you would have no way to disprove that; is that fair?
A: That's fair.

Greko Dep. 21, 25.

I

Plaintiff's complaint alleges that not only did Ms. Condon hack servers located in Dice's Bay City facility over the first two weeks of July 2011, but also over the next two weeks "Ms. Condon accessed Dice servers located at client sites and initiated file transfers of proprietary signal processing intelligence software." Second Am. Compl. ¶ 12. Ms. Condon again denies this accusation, explaining:

> In July 2011 I was asked by an employee of ESC Central to assist her in writing a report using a product known as Thoroughbred Query which can locate files within the Dice software and generate a report. It is my understanding that ESC owns the servers located in the Birmingham, Alabama office where the Query report was being run. I did not log on to the ESC servers where the Query report was being run. The login was done by the ESC employee using an ESC authorized user password.
>
> One Thoroughbred Query which I drafted related to a file known as ALSCHART. Based on my prior employment with Dice, I knew that the ALSCHART file was available for access to any customer such as ESC and I was not aware of any restriction prohibiting a Dice customer such as ESC from accessing the ALSCHART file.
>
> I did not obtain a copy of any reports generated by the Query searches run during the incident in question referred to in the complaint by Dice, nor did I provide copies of the generated reports to Bold which were solely for ESC's own use. I have never on any occasion provided Bold with a copy of the ALSCHART file.

Condon Aff. ¶¶ 3–5; *see also* Coles Aff. ¶ 7 ("Bold does not use Dice's ALSCHART codes as Bold has its own set of alarm codes that it uses.").

Plaintiff's director of software development, as noted, acknowledges that customers were permitted to query the ALSCHART file. Coppens Dep. 22–23 (quoted above). ESC Central's vice president, Ms. Jennings, confirms this. In her deposition, she was asked:

> Q: There was some claim by Mr. Dice in his deposition that this ALS[CHART] was off limits to customers. You were on that system for almost ten years. Did you ever hear anything like that before?
> A: No, never.
> Q: What was the F10 function?
> A: That was a part of the [Thoroughbred] Query function. We had actually paid for — we had actually paid Dice the year before for Amy to come down and do a training for us on Query, and it's something that we always struggled with, which is why that particular day that Amy was there she assisted in doing that whole functionality, but the ALS[CHART] codes was something that we were always in on a daily basis just about.

Jennings Dep. 48–49; *see also Dice Knowledge Base Article* 3 (Sept. 12, 2003) (user manual discussed above). Turning to why Ms. Condon assisted ESC in querying the ALSCHART file in 2011, counsel asked:

> Q: Had the data conversion from Dice to Bold been completed by the time Amy started working at Bold?
> A: Yes.
> Q: That was all done?
> A: Yes.
> Q: Okay. Did you any have any role with respect to converting the customer data from your Dice system to Bold?
> A: No. . . .
> Q: Now, just to be clear, Amy then had no role at all in converting the customer information from the old Dice system over to Bold?
> A: No.
> Q: Okay. Now did Amy assist your company with an inquiry that you wanted done regarding the ALS[CHART] file in early August?
> A: Yes.
> Q: Tell me about that.
> A: It was a query that was ran.
> Q: Okay. Who wanted the query run?

A: One of my employees, I believe.
Q: Okay. And what information did ESC want?
A: We actually had set up — upon moving off of Dice, we ran a lot of different things that we may have used then or may have used months earlier. Basically, we were just getting any information that we had that we might need in the future.
Q: I'm sorry. I really didn't follow. I mean, what — what exactly from the ALS[CHART] did you need?
A: Essentially, we — as far as the ALS[CHART] code goes, that's everywhere that I had gone in and established whether or not an operator would see the signal or if it was system handled, all of that. So we just wanted a query that was a basis of here's what we've done over the last ten years of what we've created of how we handle every signal. . . .
Q: Okay. Do you know, the day Amy assisted with the query, what login was used?
A: It was my login.
Q: Your personal login?
A: Yes.
Q: Did you give permission for that?
A: Yes.

Jennings Dep. 45–48, 51.

J

ESC Central's conversion from Plaintiff's software to Defendant's was completed in August 2011. Jennings Dep. 10. On August 5, Ms. Jennings posted a picture of herself holding two disconnected Dice cables on Facebook. Greko Dep. 37. Ms. Coppens, one of Ms. Jennings Facebook friends, saw the picture. Coppens Dep. 27. In her deposition, she was asked:

Q: Okay. So what did you do when you saw the picture?
A: I decided I needed to find out what was going on with our software.
Q: And so how did you go about doing that?
A: I went into the office and logged onto our — her system.
Q: Whose system?
A: ESC's system.
Q: And how were you able to do that, I thought she had disconnected you?
A: She actually had a web — had a phone system of ours and they did not remove access, so we were able to remote desktop into the machine, and they did not change any passwords, so you're able to log right in. . . .
Q: Okay. So why did you access her system?
A: I wanted to see what happened.
Q: Did you pick up the phone and call and ask her?

A: There's no need to call her and ask her.
Q: You didn't want to know why she unplugged your system?
A: No.

Coppens Dep. 27–28. Inquiring into what Ms. Coppens found after logging into ESC Central's system, counsel asked:

Q: Okay. And what happened next?
A: I logged into Dice and checked some files and then I went to see what queries were ran.
Q: Okay. And what did you find?
A: It appeared that queries were ran in July that could have been used to convert off of Dice.
Q: To convert what?
A: Data off Dice.
Q: You mean the customer data?
A: Yes. . . .
Q: So these queries led you to believe that ESC wanted to take its data off of the Dice software and move it to a different software, right?
A: Uh-huh.
Q: Is that a yes?
A: Yes.
Q: That is what you suspected was going on?
A: Yes.
Q: Does the customer have the right to do that?
A: Sure.

Coppens Dep. 29–30. Ms. Coppens took several screenshots of what she found before logging off ESC Central's system. In Mr. Dice's deposition, he was shown the screen shots and asked:

Q: [I]n terms of the actual data that's in these files, has any of that data, the information, the comp numbers, the identifiers, does any of that information belong to Dice or is that the customer's?
A: [It] is customer data, but again, it's — it's the — what's typed there and the extraction is very suspect because if you look at all of these as a whole — you know, you're trying to break it down one by one. That isn't what it's about. The fact that there's a thousand — there's over thousands of files and there's tens of thousands of fields and this particular site wrote some isolated queries that specifically not only took Dice property but actually systematically took exactly what was needed is an indication that the person who did this had more knowledge than a customer would.

Dice Dep. 147. Asking Mr. Dice to elaborate, counsel later asked:

Q: As I understand the overall complaint, you're not complaining that Bold took the customer data, right, you're not complaining about that?
A: No.
Q: They have the right to do that, correct?
A: It was available to them on a CIS report.
Q: You're just saying that there was a more labor-intensive way that they should have gone about doing the same thing that they did, right?
A: Yeah, exactly.
Q: And you're saying that there was a more labor-intensive way that they should have gone about doing the same thing that they did, right?
A: Yeah, exactly.

Dice Dep. 221–22. Mr. Dice's assertion, however, is in some tension with Plaintiff's own "customer implementation guide" that recommends electronic data transfer for new customers converting to Plaintiff's software, specifying:

> DICE provides three primary methods to help you populate your DICE databases: manual conversion, medium data conversion, and wire-to-wire transfer. . . .
>
> Dice usually recommends converting as much data as possible electronically . . . .
>
> *Conversion Method #2: Medium Data Conversion*
>
> Medium data conversion allows you to download database files from your old [software] system to compatible disks or tapes DICE can use. Many reasons determine why this is a good one to use, including the following:
>
> - Selection — from your existing data, you can select only the data that is necessary to transfer.
>
> - Control — you control what fields to send to DICE for conversion.
>
> - Speed — it is faster to use medium data conversion than trying to capture a report using wire-to-wire transfer.
>
> *Conversion Method #3: Wire-To-Wire Transfer*
>
> Wire-to-wire transfer captures reports from your current system into a file and then builds the data using the printed text data. As with medium data transfers, many reasons determine why this method is beneficial, including the following:
>
> - Compatibility — your current system might not have the capability to output data to a compatible disk or tape.

- Ease of use — you might not have the technical ability to format your data in a compatible format or compatible medium.

Dice Success Customer Implementation Guide 22–24 (2002) (emphasis omitted), *attached as* Def.'s Mot. Ex. E; but see Dice Aff. ¶ 7 ("Bold suggests that it is not unlawful to convert a customer's data utilizing a competitor's software and that Dice converts data in the same way. This is simply untrue. The conversion method referenced in Exhibit "E" to Bold's brief refers to the downloading of client data only.").

About ten days after Ms. Jennings posted the pictures on Facebook, Plaintiff brought suit in this Court.

K

On August 16, 2011, Plaintiff filed a complaint against Defendant asserting claims for violations of Michigan's Uniform Trade Secrets Act, conversion, and unjust enrichment. In October, Plaintiff filed its first amended complaint, adding claims for violations of the Computer Fraud and Abuse Act, the Digital Millennium Copyright Act, and copyright infringement.

In November 2011, the Court entered a stipulated order dismissing the conversion and unjust enrichment claims and permitting Plaintiff to file a second amended complaint to revise its Computer Fraud and Abuse Act claim. ECF No. 19. Plaintiff did so.

Defendant then moved to dismiss the Computer Fraud and Abuse Act claim. The motion was denied. Defendant now moves for summary judgment.

II

A motion for summary judgment should be granted if the "movant shows that there is no genuine dispute as to any material fact and that the movant is entitled to judgment as a matter of law." Fed. R. Civ. P. 56(a). The moving party has the initial burden of identifying where to look in the record for evidence "which it believes demonstrate the absence of a genuine issue of

material fact." *Celotex Corp. v. Catrett*, 477 U.S. 317, 323 (1986). The burden then shifts to the opposing party who must "set out specific facts showing a genuine issue for trial." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 250 (1986) (citation omitted). The court must view the evidence and draw all reasonable inferences in favor of the non-movant and determine "whether the evidence presents a sufficient disagreement to require submission to a jury or whether it is so one-sided that one party must prevail as a matter of law." *Id.* at 251–52.

III

Defendant moves for summary judgment on each of the four counts of the second amended complaint. Each is addressed in turn.

A

Count one of the second amended complaint alleges that Defendant violated the Michigan Uniform Trade Secrets Act, Mich. Comp. Laws §§ 445.1901–1910. Specifically, count one alleges that in July 2011 Ms. Condon misappropriated Plaintiff's trade secrets when she "initiated file transfers of proprietary signal processing intelligence software," the ALSCHART file. Second Am. Compl. ¶ 12; *see id*. ¶¶ 13–19. "Prior to its theft by Defendant in July of 2011," count one elaborates, "the signal processing intelligence at issue was neither known nor readily ascertainable by any proper means . . . . Dice protected the secrecy of this information by restricting access to this information to its employees." *Id*. ¶ 14.

The Michigan Uniform Trade Secrets Act, as its name suggests, protects a specific type of information: secret information that has commercial value. Mich. Comp. Laws § 445.1902(d); *Kubik, Inc. v. Hull*, 224 N.W.2d 80, 87 (Mich. Ct. App. 1974) ("To be a trade secret, the information must, of necessity, be a Secret"). The act defines a "trade secret" as

> information, including a formula, pattern, compilation, program, device, method, technique, or process, that is both of the following:

(i) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.

(ii) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

§ 445.1902(d); *see also Hayes-Albion v. Kuberski*, 364 N.W.2d 609, 614 (Mich. 1984) (quoting *Restatement (First) of Torts* § 757 cmt. b. (1939)).[4]

A claim of misappropriation of trade secrets has three elements: "(1) the existence of a trade secret; (2) the defendant's acquisition of the trade secret in confidence; and (3) the defendant's unauthorized use of it." *Stromback v. New Line Cinema*, 384 F.3d 283, 302 (6th Cir. 2004). In this case, Plaintiff establishes none of the three elements.

1

"The first element a plaintiff alleging misappropriation of trade secrets must prove is that the information at issue actually constitutes a trade secret." *Mike's Train House, Inc. v. Lionel, L.L.C.*, 472 F.3d 398, 410 (6th Cir. 2006). "To be a trade secret," as noted, "the information must, of necessity, be a Secret: specifically, there must be evidence presented that sufficient measures have been taken to guard the secrecy of the information and preserve its confidentiality." *Kubik*, 224 N.W.2d at 87.

In this case, the data obtained for ESC Central from the ALSCHART file in July 2011 via the Thoroughbred query was not a secret, much less Plaintiff's trade secret.

[4] The purpose of protecting trade secrets, the United States Supreme Court explains, is to "encourage invention in areas where patent law does not reach, and . . . prompt the independent innovator to proceed with the discovery and exploitation of his invention." *Kewanee Oil v. Bicron Corp.*, 416 U.S. 470, 485 (1974) (citing Gordon Doerfer, *The Limits on Trade Street Law Imposed by Federal Patent and Antitrust Supremacy*, 80 Harv. L. Rev. 1432, 1454 (1967)); *see generally Restatement (First) of Torts* cmt. a § 757 (1939) (discussing reasons for recognizing trade secret protections).

First, the information was not kept secret from customers like ESC Central. Plaintiff's user manual lists ALSCHART among the files that customers are able to query. *Dice Knowledge Base Article* 1, 3 (Sept. 12, 2003). Plaintiff's director of software development, Ms. Coppens, acknowledges that customers had unrestricted access to the ALSCHART file. In her deposition, she was asked:

> Q: It was not protected from the user, right? If you had the user login you could gain complete access to the [ALSCHART] — ALSCHART [file in July 2011], right?
> A: Yes.

Coppens Dep. 23. And Mr. Dice acknowledged in his deposition that Plaintiff's customers were not restricted from accessing the ALSCHART file (although at points in his deposition and subsequent affidavit he also takes a contrary position). He was asked:

> Q: So no administrative password would have been used —
> A: No.
> Q: — for all these queries?
> A: It just required knowledge.

Dice Dep. 159; *but see* Dice Dep. 129 (asserting that customers were not able to access the ALSCHART file); Dice Aff. ¶ 8 ("Bold also misleads this Court when it indicates that the information which Dice claims was misappropriated by Bold was readily available to Dice customers.").

Moreover, the information obtained from Ms. Condon's query of the ALSCHART file belongs to ESC Central — not Plaintiff. In Ms. Coppens' deposition, as noted, she explained that she was the person who first discovered that the queries had been run, testifying that in August 2011 "I logged into Dice and checked some files and then I went to see what queries were ran." Coppens Dep. 29. Counsel asked:

> Q: Okay. And what did you find?

A: It appeared that queries were ran in July that could have been used to convert off of Dice.
Q: To convert what?
A: Data off Dice.
Q: You mean the customer data?
A: Yes.
Q: Now the data that we are talking about, that belongs to the customer, right?
A: Specific data belongs to the customer.
Q: Just the data we're talking about that you are talking about being converted, right?
A: Yes.
Q: So these queries led you to believe that ESC wanted to take its data off of the Dice software and move it to a different software, right?
A: Uh-huh.
Q: Is that a yes?
A: Yes.
Q: That's what you suspected was going on?
A: Yes.
Q: Does the customer have the right to do that?
A: Yes.

Id. ESC Central's vice president, Ms. Jennings, confirms that the information was ESC Central's — not Plaintiff's. *See* Jennings Dep. 48 (quoted above). And Mr. Dice himself acknowledges as much. In Mr. Dice's deposition, he was asked:

Q: [I]n terms of the actual data that's in these files, has any of that data, the information, the comp numbers, the identifiers, does any of that information belong to Dice or is that the customer's?
A: [It] is customer data.

Dice Dep. 147.

In sum, the undisputed evidence shows that the information obtained from the query of the ALSCHART file in July 2011 was not a secret, much less a trade secret of Plaintiff. Plaintiff has not established the first element of a misappropriation of trade secrets claim.

2

Moreover, the information was not acquired by Defendant. As noted, the second element of a claim for misappropriation of trade secrets is "the defendant's acquisition of the trade secret in confidence." *Stromback*, 384 F.3d at 302.

In Ms. Condon's affidavit, she asserts: "I did not obtain a copy of any reports generated by the Query searches run during the incident in question referred to in the complaint by Dice, nor did I provide copies of the generated reports to Bold which were solely for ESC's own use. I have never on any occasion provided Bold with a copy of the ALSCHART file." Condon Aff. ¶ 5; *see also* Coles Aff. ¶ 7 ("Bold does not use Dice's ALSCHART codes.").

Plaintiff offers no evidence to dispute this assertion. Again, Mr. Dice himself acknowledges as much. In his deposition, he was asked:

> Q: [D]o you have any evidence that Bold is using the identical codes that Dice is using?
> A: Not until we go through all of their software and drivers.
> Q: So the answer to that question would be no, you don't?
> A: No, not at this point.

Dice Dep. 173. As the undisputed evidence is that the data queried by Ms. Condon from the ALSCHART file in July 2011 was not "acquired" by Defendant, Plaintiff has not established the second element of claim for misappropriation of trade secrets.

3

Finally, because the information is not a trade secret and has not been acquired by Defendant, Plaintiff cannot establish the final element of a misappropriation of trade secrets claim: Defendant's "unauthorized use" Plaintiff's trade secrets. *Stromback*, 384 F.3d at 302. Defendant is entitled to summary judgment on Plaintiff's misappropriation of trade secrets claim.

Arguing against this conclusion, Plaintiff asserts that there is "overwhelming evidence indicating that Bold routinely takes Dice's software and utilizes that software as a tool for converting customer data." Pl.'s Resp. 4. What this overwhelming evidence is, however, is left to the reader's imagination. Plaintiff does offer any support for its assertion.

Moreover, an independent review of the evidence put forward by the parties in this case reveals that there is no issue of fact regarding whether Defendant used Plaintiff's software in converting ESC Central's customer data: The undisputed evidence is that Defendant did not. *Compare, e.g.*, Narowski Aff. ¶¶ 6, 9 ("I did not read, review, copy, or rely upon any information about Dice source code or Dice object code when I wrote the Extraction Program, and the Extraction Program does not contain any Dice source code or object code. . . . The Extraction Program does not read or copy any source code, object code or signal processing software of Dice and is not capable of doing so."), *with* Dice Dep. 166–67, 173 (acknowledging that Plaintiff has no evidence that Defendant copied Plaintiff's source or object code).

Similarly unpersuasive is Plaintiff's conclusory assertion that "Defendant clearly obtained Dice software and used this software without permission." Pl.'s Resp. 4. Again, what the evidence is that demonstrates that Defendant "clearly obtained" Plaintiff's software is not identified. As noted, a defendant moving for summary judgment bears the initial burden of demonstrating that there is no genuine issue of fact, "but the plaintiff is not thereby relieved of his own burden of producing in turn evidence that would support a jury verdict. . . . Instead, the plaintiff must present affirmative evidence in order to defeat a properly supported motion for summary judgment. This is true even where the evidence is likely to be within the possession of

the defendant, as long as the plaintiff has had a full opportunity to conduct discovery." *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 256–57 (1986).

Defendant is entitled to summary judgment on count one of the complaint.

B

Count two of the second amended complaint alleges that Defendant violated the Digital Millennium Copyright Act, 17 U.S.C. § 1201 et seq. Specifically, count two alleges that "Dice's encryption of its software is a technological measure that effectively controls access to its products. Bold's use of former Dice employees with knowledge of methods to circumvent this encryption has permitted Bold access to Dice software without permission from Dice. Bold has utilized this unauthorized access to Dice software to unfairly compete against Dice." Second Am. Compl. ¶¶ 21–23 (formatting omitted).

The Digital Millennium Copyright Act was enacted by Congress in 1998 to "strengthen copyright protection in the digital age." *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 435 (2d Cir. 2001); *see also Chamberlain Grp., Inc. v. Skylink Techs., Inc.*, 381 F.3d 1178, 1192 (Fed. Cir. 2004) (observing that the act creates new "causes of action for liability," not new property rights).

Prohibiting the circumvention of copyright protection systems, the act provides: "No person shall circumvent a technological measure that effectively controls access to a work protected under this title." 17 U.S.C. § 1201(A)(1)(A). To "circumvent a technological measure," the act specifies, "means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner." § 1201(A)(3)(A).

"The plain language of the statute therefore requires a plaintiff alleging circumvention (or trafficking) to prove that the defendant's access was unauthorized." *Chamberlain Group*, 381 F.3d at 1193. Illustrating the rule with an analogy, the Sixth Circuit explains: "Just as one would not say that a lock on the back door of a house 'controls access' to a house whose front door does not contain a lock and just as one would not say that a lock on any door of a house 'controls access' to the house after its purchaser receives the key to the lock, it does not make sense to say that this provision of the DMCA applies to otherwise-readily-accessible copyrighted works." *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 547 (6th Cir. 2004). Rather, "the DMCA targets the *circumvention* of digital walls guarding copyrighted material (and trafficking in circumvention tools) but does not concern itself with the *use* of those materials after circumvention has occurred." *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 443 (2d Cir. 2001) (emphasis in original).

In this case, there is no evidence of unauthorized access of Plaintiff's copyrighted materials by Defendant. For example, Plaintiff's chief technical officer — the person responsible for Plaintiff's security — was asked in his deposition:

> Q: [Is there any] record or any — anything that would indicate that Amy made some type of unauthorized access to the Dice system after she left her employment?
> A: Well, as I explained earlier to you, that there's no way for me to tell. . . .
> Q: So if Amy were to deny that she ever did that, that she ever accessed the Dice server [after] she left her employment, you would have no way to disprove that; is that fair?
> A: That's fair.

Greko Dep. 21, 25. Ms. Coppens likewise acknowledges that customers were not restricted from accessing ALSCHART:

> Q: So what you are telling me about today you can't query the ALSCHART table[,] that wasn't true a year ago, right?

A: Right. A year ago you could type in the ALSCHART and the field names if you knew the field names.
Q: And it would all come up?
A: Absolutely.
Q: It was not protected from the user, right? If you had the user login you could gain complete access to the [ALSCHART] — ALSCHART table a year ago, right?
A: Yes.

Coppens Dep. 19, 22–23. Confirming this, in Mr. Dice's deposition he was asked:

Q: So no administrative password would have been used —
A: No.
Q: — for all these queries?
A: It just required knowledge.

Dice Dep. 159. Mr. Dice further acknowledged that Plaintiff's software is not encrypted. In his deposition, he was asked:

Q: [D]oes Dice . . . encrypt its software?
A: We don't have the capacity to encrypt at an object code level. We can encrypt a source code, but we've had problems with it in the past so we tend not to encrypt anything.

Dice Dep. 28; *see id*. at 81 (acknowledging "We don't have a way of encrypting files").

Ms. Condon — the person that the second amended complaint accuses of the unauthorized access — denies this accusation, explaining:

> In July 2011 I was asked by an employee of ESC Central to assist her in writing a report using a product known as Thoroughbred Query which can locate files within the Dice software and generate a report. It is my understanding that ESC owns the servers located in the Birmingham, Alabama office where the Query report was being run. I did not log on to the ESC servers where the Query report was being run. The login was done by the ESC employee using an ESC authorized user password.

Condon Aff. ¶¶ 3. ESC Central's vice president, Ms. Jennings, confirms that there was no unauthorized access of Plaintiff's copyrighted materials by Defendant:

Q: Do you know, the day [Ms. Condon] assisted with the query, what login was used?
A: It was my login.

Q: Your personal login?
A: Yes.
Q: Did you give permission for that?
A: Yes.

Jennings Dep. 51. And finally, Mr. Narowski, the gentleman who created Defendant's extraction program, explains that he has not accessed any of Plaintiff's copyrighted materials, elaborating:

> I wrote the Extraction Program using information available to the public regarding Thoroughbred Basic together with my general knowledge of computer programming. I did not read, review, copy, or rely upon any information about Dice source code or Dice object code when I wrote the Extraction Program, and the Extraction Program does not contain any Dice source code or object code. In fact, since I have been employed at Bold I have not seen a copy of Dice source code or Dice object code.

Id. ¶ 6. He emphasizes:

> The Extraction Program does not circumvent any security feature built into the Dice software. Dice has security features built into portions of its software which prevent unauthorized users from running those protected portions of the software. However, the database files where the customer data is stored are not subject to any Dice security features and can be accessed by anyone who has a copy of Thoroughbred basic, which Bold licensed from that company.

Id. ¶ 10.

In sum, there is no evidence that Defendant circumvented Plaintiff's security measures to gain unauthorized access to Plaintiff's copyrighted materials. Defendant is entitled to judgment on count two of the second amended complaint.

Opposing this conclusion, Plaintiff writes: "Mr. Narowski's deposition testimony and the Dice Affidavit both confirm that Bold's conversion software requires access to Dice software and the source code contained within that software." Pl.'s Resp. 5. Plaintiff does not assert, however, that Defendant gained unauthorized access to Plaintiff's copyrighted materials, much less offer any evidence suggesting this.

Instead, Plaintiff boldly asserts "Bold's conduct is precisely the type of 'decryption' prohibited by the DCMA." Pl.'s Resp. 5. Plaintiff does not elaborate on how Defendant allegedly decrypted Plaintiff's software, much less offer facts suggesting this. Moreover, as noted, Mr. Dice acknowledges that Plaintiff does not encrypt its software. Dice Dep. 28, 81 (quoted above).

Defendant is entitled to judgment on Plaintiff's Digital Millennium Copyright Act claim.

C

Count three of the second amended complaint alleges that Defendant willfully infringed Plaintiff's copyrights in violation of 17 U.S.C. § 106. Specifically, the complaint alleges "Bold has incorporated Dice's copyrighted software into Bold's conversion program. Bold's conversion program is a 'derivative work' as that term is defined in 17 U.S.C. § 101. Bold's derivative conversion program was created without Dice's authorization and contrary to Dice's exclusive rights to its software as provided in 17 U.S.C. § 106." Second Am. Compl. ¶¶ 26–28 (formatting omitted).

The Copyright Act gives the copyright holder "exclusive rights" to "prepare derivative works based upon the copyrighted work." 17 U.S.C. § 106(2). A "derivative work" is defined under the act as "a work based upon one or more preexisting works." § 101.

"To prevail in an action for copyright infringement," the Sixth Circuit instructs, "a plaintiff must establish that he or she owns the copyright creation, and that the defendant copied it." *R.C. Olmstead, Inc. v. CU Interface, LLC*, 606 F.3d 262, 274 (6th Cir. 2010) (quotation marks omitted) (quoting *Kohus v. Mariol*, 328 F.3d 848, 853 (6th Cir. 2003)).

Yet not all copying is actionable. The Sixth Circuit cautions that "it is a constitutional requirement that a plaintiff bringing an infringement claim must prove copying of constituent

elements of the work that are original." *Kohus*, 328 F.3d at 853 (quotation marks and emphasis omitted) (quoting *Feist Publ'ns, Inc. v. Rural Tel. Serv. Co.*, 499 U.S. 340, 361 (1991).

This can be established through either direct or indirect evidence. When the plaintiff has no direct evidence of copying, as in this case,[5] "a plaintiff must show (1) access to the allegedly-infringed work by the defendant(s) and (2) a substantial similarity between the two works at issue." *R.C. Olmstead*, 606 F.3d at 274 (quotation marks omitted) (quoting *Kohus*, 328 F.3d at 853).

Because only original elements are protected, however, "before comparing similarities between two works a court should first identify and eliminate those elements that are unoriginal and therefore unprotected." *R.C. Olmstead*, 606 F.3d at 274 (citing *Kohus*, 328 F.3d at 853). After distilling the work to protected elements, the court must then determine "whether the second work involves elements that are substantially similar to the protected elements of the original work." *R.C. Olmstead*, 606 F.3d at 274 (citing *Kohus*, 328 F.3d at 855). The Sixth Circuit refers to this as an "abstraction-filtration-comparison analysis." *R.C. Olmstead*, 606 F.3d at 274 (citing *Kohus*, 328 F.3d at 855).

In *R.C. Olmstead*, for example, the plaintiff brought a copyright infringement claim alleging that the defendant had copied the plaintiff's software. 606 F.3d at 268. In support of its claim, the plaintiff produced the testimony of an expert, Robert Reid, and nearly two hundred pages of exhibits comparing the two companies' software. *Id*. at 267. The district court excluded the expert's testimony, explaining "Reid woefully fails to provide any reasoning or logical support for his conclusions. Reid vaguely lists a sampling of 'similarities' between the [plaintiff's] and [the defendant's] softwares, but he never explains why the alleged similarities

[5] *See, e.g.*, Narowski Aff. ¶¶ 6, 8–10 (quoted above); Narowski Supp. Aff. ¶ 7 ("During the conversion process Bold does not utilize any Dice source code nor does it run any of the Dice software programs, such as the Dice receiver driver programs."), *attached as* Def.'s Reply Ex. Z.

indicate actual copying of Plaintiff's software rather than that the softwares simply perform similar functions (and thus would be expected to function similarly)." *Id*. at 268. The court then granted the defendant summary judgment on the copyright infringement claim. The Sixth Circuit affirmed, writing:

> [The plaintiff] has not attempted to identify any original elements of its software that [the defendant] copied. Because [the plaintiff] has failed to produce evidence creating a question of fact as to whether [the defendant] copied original elements of its software, [the defendant] was entitled to summary judgment on [the plaintiff's] copyright infringement claims.

Id. at 275. Writing in the alternative, the court noted that even if the expert's testimony had not been excluded, the defendant would nevertheless be entitled to summary judgment:

> Neither Reid's report, nor Reid's additional declaration provided by Olmstead in an attempt to cure the deficiencies in the report, even begins to provide the kind of abstraction-filtration-comparison analysis we applied in *Kohus* and that the district court found lacking. As mentioned above, under *Kohus*, the factfinder determines substantial similarity first by asking what aspects of the copyrighted work, if any, are protected, and then by asking whether the second work involves elements that are substantially similar to the protected elements of the copyrighted work. All of the evidence offered by [the plaintiff] clearly lacks the abstraction and filtration elements. [The plaintiff] has not attempted to identify those elements of its software that are original; thus its substantial similarity analysis does not filter elements that would be expected to be common to any credit union software, those dictated by the particular business practices.

Id. (citations omitted) (citing *Kohus*, 328 F.3d at 855 & 855 n.1).

In this case, as in *R.C. Olmstead*, Plaintiff does not attempt to identify any original elements of its software that Defendant allegedly copied. Unlike *R.C. Olmstead*, moreover, Plaintiff does not even offer a comparison of the software of the respective companies.

Instead, Plaintiff tersely alleges that "loading validly copyrighted software onto a computer without the owner's permission, then using the software for the principal purpose for which it was designed is a form of copyright infringement. Bold's Matt Narowski admits that this precisely how his conversion program operated." Pl.'s Resp. 5–6 (citation and quotation

marks omitted) (quoting *R.C. Olmstead, Inc. v. CU Interface, LLC*, 657 F. Supp. 2d 878, 890 (N.D. Ohio 2009) *aff'd*, 606 F.3d 262 (6th Cir. 2010).

Contrary to Plaintiff's contention, Mr. Narowksi acknowledges no such thing. In his affidavit, as noted, he explains:

> The function of the Extraction Program is to extract the customer data from databases stored on the Linux operating platform used by Dice software. The customer data is extracted in a comma-separated text file, which is a format that Bold uses to convert the customer data into Manitou . . . .
>
> The Extraction Program is not capable of operating an alarm company central station or of monitoring or processing an alarm signal, which is my general understanding of the function of the Dice software.

Narowski Aff. ¶¶ 7–8. Discussing how he created the extraction program, Mr. Narowski continues:

> I wrote the Extraction Program using information available to the public regarding Thoroughbred Basic together with my general knowledge of computer programming. I did not read, review, copy, or rely upon any information about Dice source code or Dice object code when I wrote the Extraction Program, and the Extraction Program does not contain any Dice source code or object code. In fact, since I have been employed at Bold I have not seen a copy of Dice source code or Dice object code.

Id. ¶ 6. And he emphasizes: "The Extraction Program does not read or copy any source code, object code or signal processing software of Dice and is not capable of doing so." *Id*. ¶ 9.

In his deposition, Mr. Narowski did acknowledge he had received an external hard drive from another of Plaintiff's former clients (Sonitrol) when it transferred its business to Defendant. *See* Narowski Dep. 49–50. He emphasized however, that he did not use any of Plaintiff's software for the principal purpose for which it was designed (alarm monitoring), explaining:

> The "Dice Data" that I was referring to was data that was owned by [the client] regarding its subscribers that was stored in the databases that were on the hard drive I received for the purpose of converting the customer data from Dice software into Bold. . . . I do not know exactly what was included on the hard

> drive that [the customer] sent me. My concern was that the hard drive contain all of the customer data that [the client] needed converted. . . .
>
> During the conversion process Bold does not utilize any source code nor does it run any of the Dice software programs, such as the Dice receiver driver programs. Bold has never used Dice software for the purpose of monitoring alarm signals.

Narrowski Supp. Aff. ¶ 3, 7. Plaintiff offers no evidence to dispute this.

As the undisputed evidence is that Defendant did not use Plaintiff's software, much less use it for the principal purpose for which it was designed, Defendant is entitled to summary judgment on Plaintiff's copyright infringement claim.

D

Count four of the second amended complaint alleges that Defendant violated the Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030. Specifically, the complaint alleges: "The Dice servers accessed by Bold are used in both interstate and foreign commerce and are thus 'protected computers' as defined at 18 USC § 1030(e)(2). Bold's access to confidential and proprietary information contained on the Dice servers was both intentional and without authorization. Dice has sustained a 'loss' significantly in excess of $5,000." Second Am. Compl. ¶¶ 32–34 (formatting omitted).

The Computer Fraud and Abuse Act, the "first Federal computer crime statute," S. Rep. 104–357, at 3 (1996), had its genesis in the enactment of "a massive omnibus crime bill known as the Comprehensive Crime Control Act [of 1984, Pub. L. No. 98–473, 98 Stat. 1976]." Orin Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1563 (2010).

Codified at 18 U.S.C. § 1030, it criminalized "three specific [actions]: computer misuse to obtain national security secrets, computer misuse to obtain personal financial records, and

hacking into U.S. government computers." *Id*. at 1564 (citing 18 U.S.C. § 1030(a)(1)–(3)). Two years later, Congress criminalized three more computer activities:

> Section 1030(a)(4) prohibited unauthorized access with intent to defraud; essentially, the traditional crime of wire fraud committed using a computer. Section 1030(a)(5) prohibited accessing a computer without authorization and altering, damaging, or destroying information, thereby causing either $1,000 or more of aggregated loss . . . . Section 1030(a)(6) prohibited trafficking in computer passwords.

Kerr, *supra*, at 1565 (footnotes omitted). Eight years passed. In 1994, Congress enacted another omnibus crime bill, the Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103–322, 108 Stat. 1796. Although better known for its provisions regarding a federal assault weapons ban, the bill also included the Computer Abuse Amendments Act, which added civil remedies for violations of § 1030. *See generally* Deborah F. Buckman, *Validity, Construction, and Application of Computer Fraud and Abuse Act*, 174 A.L.R. Fed. 101 (2001).

"Any person who suffers damage or loss by reason of a violation of the section," subsection (g) provides in pertinent part, "may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

In this case, as noted, the second amended complaint alleges that Defendant violated the act when Ms. Condon accessed Plaintiff's servers during July 2011. *See* Second Am. Compl. ¶¶ 12, 31–34. Ms. Condon unequivocally denies doing so. Condon Aff. ¶ 6 ("Since I terminated my employment at Dice [in May 2011], I have never accessed or attempted to access any server owned by Dice at its Bay City office or any other location."). And Mr. Dice acknowledges that Plaintiff has no evidence that Ms. Condon accessed Dice servers. In his deposition, he was asked:

Q: Are you claiming that Amy Condon hacked into the Dice servers in Bay City Michigan, yes or no?
A: I don't think she hacked into anything. I don't — I don't know if she did or not. . . .
Q: Did any Bold employees hack into Dice servers located in Bay City, Michigan?
A: I don't know how Bold got our — got all of our intelligence. . . . It's not a question for me to answer, it's a question for you to answer. How did Bold get access to those files[?] . . .
Q: So the answer to the question that I asked you is you don't know if some Bold employees hacked into the Dice servers located in Bay City, Michigan?
A: I don't know how Bold got the information to be able to do what they've done. I have no idea. All I know is that they have it. . . .
Q: Okay. I want to know [about] is this sentence [in paragraph twelve of the complaint] claiming that after Ms. Condon left her employment at Dice she somehow hacked into Dice's Bay City servers?
A: That's what that says . . . .
Q: All right. So on what dates did Miss Condon hack into the servers located in Dice's Bay City facility; what dates did that happen?
A: We don't know.
Q: Okay. How did she hack into the system?
A: We don't know.

Dice Dep. 35–41. Plaintiff's chief technical officer, the person directly responsible "for maintaining the security of the Dice servers in Bay City," confirms that Plaintiff has no evidence that any of Defendant's employees accessed Plaintiff's servers. Grecko Dep. 12, 21, 25. In his deposition, the gentleman was asked:

Q: Are you aware of any evidence, do you have any fact that you could point to to say that [Ms. Condon] actually accessed the Dice servers in Bay City, Michigan after she left the company?
A: No, there's no proof I can give you saying here's a document to say Amy did X, Y, Z.
Q: And there's no record or any — anything that would indicate that Amy made some type of unauthorized access the Dice system after she left her employment?
A: Well, as I explained earlier to you, that there's no way for me to tell. . . .
Q: So if Amy were to deny that she ever did that, that she ever accessed the Dice server [after] she left her employment, you would have no way to disprove that; is that fair?
A: That's fair.

Greko Dep. 21, 25. Because there is no evidence that Defendant accessed Plaintiff's servers, Defendant is entitled summary judgment on count four of the second amended complaint.

Against this conclusion, Plaintiff writes that it is not Ms. Condon but Mr. Narowski who accessed Plaintiff's servers. Pl.'s Resp. 6. (Mr. Narowski is not mentioned in either the original complaint, the first amended complaint, or the second amended complaint.) Plaintiff attaches an email Mr. Narowski sent to another alarm company, Doyle Security, that was converting from Plaintiff's software to Defendant's system. Pl.'s Resp. Ex. E, at 4. "I can do a gotoassist session with you," Mr. Narowski wrote, "and we can login on the DICE server to find out if that works for you." *Id*.

In isolation, this email appears to support Plaintiff's argument. Yet as Judge Learned Hand cautioned, "There is no surer way to misread any document than to read it literally." *Guiseppi v. Walling*, 144 F.2d 608, 624 (2d Cir.1944) (L.Hand, J., concurring).

Explaining what the reference to a "dice server" meant, Mr. Narowski explains that it was shorthand for the Doyle Security server running Plaintiff's software during the conversion process — not one of Plaintiff's servers, elaborating:

> During the phase of the conversion process where the customer is running the Dice software on one server in parallel to the Bold software on another server, we will often call the server running Dice the "Dice Server" and the server running Manitou the "Bold Server" or the "Manitou Server" even though both servers are owned by the customer, not Dice or Bold. The "Dice Server" that I was referring to [in the email Plaintiff relies on] was a server owned by Doyle which was part of the Doyle computer system that was running Dice software. As far as I am aware this server was not connected to the Dice computer system in Bay City[,] Michigan. In my email to Mr. Ritch I was explaining the capability of the GoToAssist function and I do not recall if I ever accessed the Doyle server running Dice software using GoToAssist. I have never used GoToAssist to access any server owned by Dice.

Narowski Supp. Aff. ¶ 4; *see also* Condon Supp. Aff. ¶ 4 (asserting that she did not use the GoToAssist function to access Dice servers). Plaintiff offers no evidence to dispute this. On the

contrary, as noted, Plaintiff acknowledges that it does not know whether Defendant has ever accessed Plaintiff's servers.

Defendant is entitled to summary judgment on count four of the second amended complaint.

IV

Accordingly, it is **ORDERED** that Defendant's motion for summary judgment (ECF No. 61) is **GRANTED**.

Is further **ORDERED** that the motion to bar plaintiff from presenting damages evidence (ECF No. 49), motion in limine (ECF No. 65), motion to strike (ECF No. 86), motion for sanctions (ECF No. 88) and motion for continuance (ECF No. 92) are **DENIED AS MOOT**.

Is further **ORDERED** that the second amended complaint is **DISMISSED WITH PREJUDICE**.

Dated: October 25, 2012

s/Thomas L. Ludington
THOMAS L. LUDINGTON
United States District Judge

PROOF OF SERVICE

The undersigned certifies that a copy of the foregoing order was served upon each attorney or party of record herein by electronic means or first class U.S. mail on October 25, 2012.

s/Tracy A. Jacobs
TRACY A. JACOBS