

*To Be Published:*

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF IOWA  
EASTERN DIVISION**

SERVERSIDE GROUP LIMITED and  
SERVERSIDE GRAPHICS, INC.,

Plaintiffs,

vs.

TACTICAL 8 TECHNOLOGIES,  
L.L.C., and BANK IOWA  
CORPORATION,

Defendants.

No. C 12-2016-MWB

**MEMORANDUM OPINION AND  
ORDER REGARDING PLAINTIFFS'  
MOTION FOR PARTIAL  
RECONSIDERATION OF SUMMARY  
JUDGMENT ORDER**

---

This patent-infringement action, alleging infringement of two of the plaintiffs' patents, U.S. Patent No. 7,931,199 (the '199 patent) and U.S. Patent No. 7,946,490 (the '490 patent), both entitled "Computerized Card Production Equipment," is before me on the December 12, 2013, Motion For Partial Reconsideration Of Summary Judgment Order (docket no. 151) by plaintiffs Serverside Group Limited and Serverside Graphics, Inc., collectively "Serverside." Because trial in this matter is set to begin on January 21, 2014, I entered an Order (docket no. 152) on December 20, 2013, setting expedited briefing deadlines and telephonic oral arguments on Serverside's Motion For Partial Reconsideration. Defendants Tactical 8 Technologies, L.L.C., now known as Banno, L.L.C. (Banno), and Bank of Iowa Corporation (BIC), collectively "the Iowa Defendants," filed their Resistance (docket no. 155) on December 30, 2013, and Serverside filed its Reply (docket no. 162) on January 2, 2014. I heard telephonic oral

arguments on the Motion on January 3, 2014. I have expedited my disposition of the Motion, as well.

Serverside seeks reconsideration of pages 64-66 and 75-77 of my December 9, 2013, Memorandum Opinion And Order Regarding Defendants' Motion for Summary Judgment (Summary Judgment Ruling) (docket no. 144), *Serverside Group Ltd. v. Tactical 8 Techs., L.L.C.*, \_\_\_ F. Supp. 2d \_\_\_, \_\_\_, 2013 WL 6448824, \*30-\*31, \*36-\*37 (N.D. Iowa Dec. 9, 2013). In the first cited section of my Summary Judgment Ruling, I concluded that, as to the "secure unique identifier" of claim 1 of the '199 patent, "it is not the *system* that must be 'secure,' but the 'unique identifier' *itself* that must be 'secure'"; that, as to the "uniqueness" requirement, the Iowa Defendants had pointed to evidence that there is a possibility, however small or remote, that two customers of the same financial institution could have the same first and last names and the same last four digits of their PANs, that Serverside had failed to generate a genuine issue of material fact that the Gramm–Leach Bliley Act Standards For Safeguarding Customer Information or pertinent regulations would preclude such an occurrence, or that such an occurrence is computationally impossible; and that, as a consequence, the Iowa Defendants were entitled to summary judgment of noninfringement of claim 1 of the '199 patent, because Serverside had not generated any genuine issue of material fact that there was any "secure" or "unique" identifier in Banno's accused Cre8MyCard system. Summary Judgment Ruling at 64-66, *Serverside Group Ltd.*, \_\_\_ F. Supp. 2d at \_\_\_, 2013 WL 6448824 at \*30-\*31 (emphasis in the original).

In the second cited section of my Summary Judgment Ruling, I reached a similar conclusion that, as to the "encrypted customer information" limitation of the claims of the '490 patent, "it is not the system, but the 'customer identifier' itself that must 'encompass [ ] encrypted customer information,'" and that, as a consequence, the Iowa Defendants were entitled to summary judgment that they do not infringe claim 1 of the

'490 patent, and all other patent claims of the '490 patent at issue, as a matter of law, because Serverside had failed to generate a genuine issue of material fact that the alleged "customer identifier" in the Cre8MyCard system "encompasses encrypted customer information." *Id.* at 75-77, *Serverside Group Ltd.*, \_\_\_ F. Supp. 2d at \_\_\_, 2013 WL 6448824 at \*36-\*37.

I turn, first, to the questions of the authority and standards for reconsideration of these conclusions in my Summary Judgment Ruling. In *Kirt v. Fashion Bug # 3252, Inc.*, 495 F. Supp. 2d 957 (N.D. Iowa 2007), I addressed these questions, as follows:

This court has previously found that Rule 54(b) of the Federal Rules of Civil Procedure provides authority for a court to reconsider any interlocutory order, including a prior ruling on a motion for summary judgment. *Doctor John's, Inc. v. City of Sioux City, Iowa*, 467 F. Supp. 2d 925, 931 (N.D. Iowa 2006); *Wells' Dairy, Inc. v. Travelers Indemnity Company of Illinois*, 336 F. Supp. 2d 906, 909 (N.D. Iowa 2004) (citing cases). Specifically, Rule 54(b) provides that, unless the court certifies the order for interlocutory appeal, "any order or other form of decision, however designated, which adjudicates fewer than all the claims or the rights and liabilities of fewer than all the parties shall not terminate the action as to any of the claims or parties, and the order or other form of decision is subject to revision at any time before the entry of judgment adjudicating all the claims and the rights and liabilities of all the parties." Fed. R. Civ. P. 54(b) (emphasis added). Moreover, this court has repeatedly held that it has the inherent power to reconsider and revise any interlocutory order, such as a summary judgment ruling, up until the time that a final judgment is entered. *Wells' Dairy, Inc.*, 336 F. Supp. 2d at 909 (citing *Kaydon Acquisition Corp. v. Custum Mfg., Inc.*, 317 F. Supp. 2d 896, 903 (N.D. Iowa 2004); *Helm Financial Corp. v. Iowa N. Ry. Co.*, 214 F. Supp. 2d 934, 999 (N.D. Iowa 2002); and *Longstreth v. Copple*, 189 F.R.D. 401, 403 (N.D. Iowa 1999)).

This court has also noted, “The exact standard applicable to the granting of a motion under Rule 54(b) is not clear, though it is typically held to be less exacting than would be [applicable to] a motion under Federal Rule of Civil Procedure 59(e), which is in turn less exacting than the standards enunciated in Federal Rule of Civil Procedure 60(b).” *Id.* Although the standards for reconsideration of interlocutory orders may be less “exacting” than the standards for reconsideration of final orders under Rules 59(e) and 60(b), this court has nevertheless held that it should look to the general principles under Rules 59(e) and 60(b) for guidance when reconsidering a summary judgment ruling pursuant to Rule 54(b). *Id.* (citing *Bragg v. Robertson*, 183 F.R.D. 494, 496 (S.D. W. Va. 1998)). Under Rule 59(e), a judgment may be amended to correct “clearly” or “manifestly” erroneous findings of fact or conclusions of law. *See, e.g., Hagerman v. Yukon Energy Corp.*, 839 F.2d 407, 414 (8th Cir. 1988); *Baker v. John Morrell & Co.*, 266 F. Supp. 2d 909, 919 (N.D. Iowa 2003). It is this standard that the court finds is applicable to reconsideration of a summary judgment ruling under Rule 54(b).

*Kirt*, 495 F. Supp. 2d at 964–65; *see also Rattray v. Woodbury Cnty., Iowa*, 908 F. Supp. 2d 976, 984-85 (N.D. Iowa 2012) (quoting this portion of *Kirt*). I conclude that these standards are also applicable to Serverside’s Motion For Partial Reconsideration of my Summary Judgment Ruling.

The first error in my Summary Judgment Ruling that Serverside asserts is that it was improper for me to grant summary judgment on the basis of arguments or issues not raised by the parties in their arguments concerning summary judgment or that had not previously been part of the case. The Eighth Circuit Court of Appeals has stated,

We have repeatedly held that in the Eighth Circuit, a district court commits reversible error when it grants summary judgment on an issue not raised or discussed by the parties. It is fundamentally unfair to the nonmoving party to require

her to address issues not addressed by the moving party in anticipation that the district court might rely on some unidentified issue to grant the motion.

*Heisler v. Metropolitan Council*, 339 F.3d 622, 631 (8th Cir. 2003); *see also Cowden v. BNSF Ry. Co.*, 690 F.3d 884, 895 (8th Cir. 2012) (quoting this excerpt from *Heisler*); *Liberty Mut. Ins. Co. v. Pella Corp.*, 650 F.3d 1161, 1178 (8th Cir. 2011) (also quoting this excerpt from *Heisler*). Leaving aside—for the moment—the question of whether I granted summary judgment in the challenged portions of my Summary Judgment Ruling on the basis of grounds not raised or discussed by the parties or previously part of the case, as Serverside contends, Serverside now concedes that, by entertaining briefing and oral arguments on its Motion For Partial Reconsideration, I have remedied any fundamental unfairness in the challenged parts of my Summary Judgment Ruling and that I may now enter rulings on the pertinent issues either altering or adhering to my previous rulings.

Thus, the real question on Serverside’s Motion For Partial Reconsideration is whether I “clearly” or “manifestly” erred, as a matter of fact or law, in my conclusions in the challenged parts of my Summary Judgment Ruling. *See Kirt*, 495 F. Supp. 2d at 965. I conclude that I did not, even considering Serverside’s additional arguments in support of its Motion For Partial Reconsideration.

More specifically, Serverside argues that, contrary to my Summary Judgment Ruling, neither the claims, the specification, nor my prior constructions of the claim terms at issue require that the “security” of the “secure unique identifier” in claim 1 of the ‘199 patent, or the “encryption” of customer information in the customer identifier in claim 1 of the ‘490 patent, be intrinsically “secure” (or “encrypted”). Rather, Serverside argues that such “security” or “encryption” can be achieved in a variety of ways, including firewall trust security, secure locations, encrypted transmissions, etc.

Serverside cites in support of this contention portions of the '199 patent at 9:60-10:11; 10:62-11:46; 15:19-16:4; 17:8-22.

What is conspicuous by its absence from each of these cited portions of the specification, however, is any reference to the “customer identifier” or “customer information” being “secure” or “encrypted” by the system or only when transmitted to the system’s server by means of SSL internet encryption, even where they refer to the “customer identifier” as being “unique.” Indeed, the only excerpt that even mentions the customer identifier being “secure” is the last one, which states the following:

The blank stock printer may then print **1223** the image onto blank stock, and encode the card’s magnetic strip. Based on information in the magnetic strip, the emboss record and printed card stock may then be joined together **1224** to create a finished card.

In an alternative to the embodiment of FIGS. **11** and **12**, which utilize a unique identifier and a hash value, respectively, other methods of creating a secure user identifier may be used. For example, it is also possible for the user information to be encrypted at the card issuer at the beginning of the process, and decrypted at the card bureau using a Private/Public Key or a Private/Private Key encryption technology. This alternative works in a manner similar to the process described in FIG. **12**, but with modified security measures; for example, the key must be held by the card bureau.

The '199 patent, 17:8-22. This excerpt, however, explains that the user information is “encrypted at the card issuer at the beginning of the process,” *i.e.*, before the customer even begins to customize a card, not merely when the customer’s user information and card customization information are transmitted to the system’s server. Furthermore, “[t]his alternative works in a manner similar to the process described in FIG. **12**.” In the “process described in FIG. **12**,” “a ‘hash value’ (or other one-way code) is passed between the card issuer **1204** and the back end server **1203**, instead of requiring the

card issuer to create a unique identifier for each customer, as in FIG. 11.” The ‘199 patent, 16:18-21. This excerpt confirms that the “encrypted” user information, described in the ‘199 patent, 17:8-22, is created by the card issuer and “passed between the card issuer and the back end server”; the “encryption” does not occur merely when the customer uploads his or her information or identifier and card customization information to the system’s server.

Next, Serverside argues that dependent claims 3 and 4 of the ‘199 patent, which claim the invention in claim 1 “wherein the customer identifier comprises a machine readable code” and a “barcode,” respectively, do not use identifiers that are truly “secure” in and of themselves, but only to the extent that the identifier contained within them has already been made secure, through encryption, firewall trust security, etc. The fact that “machine readable code” and a “barcode” can be “read” by appropriate computer programs or even by the human eye, however, does not mean that they are not “secure” in and of themselves, because merely “reading” them would not “decrypt” or render “insecure” the information that they represent.

Furthermore, perhaps the clearest indication that it is the “identifier” itself that must be “secure” or “encrypted” comes from the precise part of claim 1 of both patents that Serverside relies on to attempt to prove the opposite. Serverside argues that, because claim 1 of both patents claims “a module configured to receive a customer identifier . . . wherein the customer identifier [comprises . . . a secure unique identifier/encompasses encrypted customer information],” it plainly does not require that the customer identifier itself be “secure” or “encrypted” when created, but only that the customer identifier be “secure” or “encrypted” when it is *received* by the system, such as by transmission of the customer identifier to the system (or the Banno server) using standard SSL internet encryption. The cited limitations of claim 1 are the following:

a module configured to receive a customer identifier that corresponds to the remote customer that personalized said image;

\* \* \*

wherein the customer identifier comprises an identifier selected from a secure unique identifier and a one-way code.

The '199 patent, claim 1. Contrary to Serverside's argument, the separation of the very last limitation of claim 1, claiming a "customer identifier" that is a "secure unique identifier," from the earlier limitation, claiming "a module configured to receive a customer identifier," plainly demonstrates that the "security" of the "unique identifier" is part of the "unique identifier" itself, not merely something that happens to the "unique identifier" when it is transmitted from the customer to the module of the system that is configured to receive it. Specifically, this limitation plainly indicates that, where the "customer identifier" is a "secure unique identifier," the "security" of the "unique identifier" occurred separately from and prior to its transmission via the internet to the receiving module and that all other references to "the customer identifier" or "said customer identifier" in claim 1 are to the "customer identifier" that is *already, itself*, a "secure unique identifier" or a "one-way code."<sup>1</sup>

---

<sup>1</sup> This reading is reinforced, as the Iowa Defendants contend, by another separate limitation of claim 1, which claims "a controller operable, based on *said customer identifier*, to cause printing of said personalized customer image onto the card material and to cause application of relevant financial information from the financial record onto the card material." The '199 patent, claim 1 (emphasis added). This limitation also plainly indicates that, where the "customer identifier" is a "secure unique identifier," the "security" of the "unique identifier" occurred separately from and prior to its transmission via the internet to the card printer and that all other references to "the

(Footnote continued . . .

Also, as to the “secure” part of the “secure unique identifier” limitation, I reiterate my conclusion from my *Markman* ruling that “the ‘secure unique identifier’ is *a specific kind* of ‘customer identifier,’” and that, consequently, it should be construed as “a secure, unique signal, character, or group of characters that can be used to identify the customer.” *Serverside Group, Ltd.*, 927 F. Supp. 2d at 660 (emphasis added). My assertion in my Summary Judgment Ruling that it is the “customer identifier” *itself* that must be “secure” is implicit in this construction from my *Markman* ruling, so that this construction of the “customer identifier” as *itself* “secure” should have come as no surprise to Serverside. Thus, as I pointed out in my Summary Judgment Ruling, it was the parties who were attempting to introduce new constructions of the “secure” limitation, while losing sight of the fact that it is not the system that must be “secure” or “encrypted,” but the identifier *itself*. *Serverside Group, Ltd.*, \_\_\_ F. Supp. 2d at \_\_\_, 2013 WL 6448824 at \*30 and \*36. I did not base this conclusion on grounds that had never been part of the case, as Serverside now contends, but on a construction of the claim terms that had been part of the case since my *Markman* ruling.

Furthermore, because the “one-way code,” the other alternative for a “customer identifier” in claim 1 of the ‘199 patent, would also be “secured” or “encrypted” by standard SSL internet encryption when transmitted from the customer to the system, if that is all that “secure” and “encrypted” mean, then “secure” and “encrypted” become entirely superfluous as distinctions between the “secure unique identifier” and “encrypted customer information,” on the one hand, and the “one-way code,” on the other. It is my constructions of “secure unique identifier” and “encrypted customer information”—as meaning that the “unique identifier” *itself* must be “secure” in the

---

customer identifier” or “said customer identifier” in claim 1 are to the “customer identifier” that is *already* a “secure unique identifier” or a “one-way code.”

‘199 patent, and that the “customer information” *itself* must be “encrypted” to make the “customer identifier” claimed in the ‘490 patent, not merely that the *system* must be “secure” or use some form of “encryption”—that create the proper differentiation between these alternative limitations. *See, e.g., Kraft Food, Inc. v. International Trading Co.*, 203 F.3d 1362, 1365-69 (Fed. Cir. 2000) (explaining that there is a presumption that two independent claims have different scope when different words or phrases are used in those claims).

In short, contrary to Serverside’s contentions, my conclusions in the challenged parts of my Summary Judgment Ruling that the “unique identifier” *itself* must be “secure” and that the “customer information” *itself* must be “encrypted” are entirely consistent with the specification of the patents, the claims of the patents-in-suit, and my prior constructions of those claim terms.

Finally, turning to the “unique” limitation, Serverside argues that the Iowa Defendants have not submitted any evidence that there has ever been an instance in which two customers share both first and last names and the last four digits of their PANs, so that “customer identifiers” derived from this information are “unique” within the ordinary meaning of the term. More specifically, Serverside argues that the possibility (which it contends is extremely remote) that a “clone” of a “customer identifier” derived in this way could occur does not fit with the ordinary meaning of “unique,” on which my claim construction relied, because the customer identifier is “unique” until such a “clone” actually appears. Even if there has been an instance in which “clones” have actually occurred, Serverside argues that such occurrences could, at most, very slightly reduce the potential damages base, because infringement occurs if the system is *capable* of operating in an infringing mode.

I believe that this argument is in error, because it confuses infringement with claim construction. As a matter of claim construction, in the *Markman* ruling, I

contrasted a “unique” value, or one that was “impossible” to generate from two different input strings, with one for which there was an “infinitesimally small” chance, or for which it was merely “computationally infeasible,” that different input strings would generate the same value. *See Serverside Group, Ltd.*, 927 F. Supp. 2d at 673. Indeed, this construction of “unique” as meaning that exact copies or “clones” are “impossible” comports with the ordinary meaning of “unique” as “being the only one,” or “being without a like or equal,” or “distinctively characteristic,” *i.e.*, “being the only one” *ever*, not just “being the only one” *as yet*. MERRIAM WEBSTER’S COLLEGIATE DICTIONARY (10th ed. 1995), 1292 (definitions of “unique”).<sup>2</sup> Furthermore, if, as I concluded in my Summary Judgment Ruling, the “customer identifier” in the accused system is not “unique” within this construction, because it is possible that a different input string would generate the same value, the “customer identifier” of the accused system *never* infringes the “unique customer identifier” limitation of the patent, because it *never* embodies the claimed invention. This is different from an accused system that only sometimes embodies the claimed invention or sometimes operates in an infringing mode. *See* Summary Judgment Ruling at 44-45; *Serverside Group, Ltd.*, \_\_\_ \_\_\_ F. Supp. 2d at \_\_\_, 2013 WL 6448824 at \*19-\*20. Serverside failed to generate a genuine issue of material fact that it is impossible for the accused system to generate the same “customer identifier” from different input strings,

---

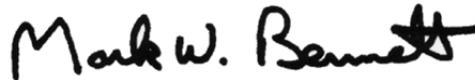
<sup>2</sup> For example, Serverside argues that Mount Rushmore is “unique,” because no one has yet built an exact copy of it. Serverside’s Reply (docket no. 162), 5. Without getting carried away into a discussion of aesthetics, suffice it to say that even a “copy” of Mount Rushmore would not render the original any less “unique,” because no “exact” copy is possible. Here, an “exact” copy or “clone” of a “customer identifier” derived from the first and last names of the customer and the last four digits of his or her PAN is possible.

such that the “customer identifier” is “unique.” Consequently, Serverside has failed to generate a genuine issue of material fact that the accused system *ever* infringes the “unique identifier” limitation.

THEREFORE, Serverside’s December 12, 2013, Motion For Partial Reconsideration Of Summary Judgment Order (docket no. 151) is **granted**, to the extent that I have provided the parties with the opportunity to brief and argue the grounds on which I purportedly *sua sponte* based the challenged parts of my Summary Judgment Ruling, but having done so, the Motion is **denied**, to the extent that I find no reason to alter the challenged parts of my Summary Judgment Ruling.

**IT IS SO ORDERED.**

**DATED** this 6th day of January, 2014.



---

MARK W. BENNETT  
U.S. DISTRICT COURT JUDGE  
NORTHERN DISTRICT OF IOWA