UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

FINANCIAL INFORMATION TECHNOLOGIES, LLC,

Plaintiff,

Case No.: 8:17-cv-00190-T-23MAP

vs.

ICONTROL SYSTEMS, USA, LLC,

Defendant.
_____/

iCONTROL'S RESPONSE TO PLAINTIFF'S
RENEWED MOTION FOR PERMANENT INJUNCTION

Fintech's original injunction motion asked this Court to enter a sweeping permanent injunction that would have prohibited iControl "from doing business in the regulated commerce industry." Doc. 249 at 5. That motion was overreaching and improper. As the Court explained in denying the motion on August 10, 2020, "the Florida Uniform Trade Secrets Act authorizes the injunction of ***specific, identifiable*** trade secrets but authorizes no blanket restraint of competition." Doc. 279 at 3 (emphasis added). The Court had no obligation to give Fintech any opportunity to seek a narrower injunction. After all, Fintech had chosen—for its own strategic reasons—to seek only a blanket restraint on competition. Fintech had put all its eggs in that basket and had not asked for a narrower injunction, not even in the alternative. The Court, however, generously gave Fintech ***one week***—until August 17—to file a second motion for a permanent injunction that would "identify[] ***with reasonable particularity*** the ***specific*** trade secrets for which Fintech requests an injunction." *Id.* at 4 (emphasis added).

Fintech has flouted the Court's order in multiple ways. ***First***, Fintech failed to renew its motion by the deadline the Court imposed. Fintech's attempt to blame that failure on a calendaring

error is misdirection: The deadline was *only seven days away*, so Fintech's lawyers should not have needed the deadline calendared to keep it in mind. The real issue is that none of Fintech's multiple lawyers could be bothered to *read* the four-page order, at least not carefully enough to register the "[n]o later than" deadline set out in bold capital letters. It is well established that an attorney's failure to read and comprehend a court order is not excusable neglect.

Second, Fintech's renewed motion fails on the merits because it does not identify with reasonable particularity the specific trade secrets at issue. Instead, Fintech seeks to enjoin iControl in such broad, vague, and confusing terms that iControl will have no way of determining whether it is in compliance and will have to expose itself to the risk of contempt in order to compete with Fintech in the regulated commerce industry. Fintech's proposed injunction can only be intended to force iControl to exit the regulated commerce business altogether—exactly the result Fintech sought to achieve with its original motion—which would have a devastating impact not only on iControl and its employees, but also on iControl's thousands of innocent customers. iControl still does not understand what specific trade secrets Fintech is claiming or what specific conduct the proposed injunction would prohibit.

Besides being legally improper, Fintech's repeated demands for overly broad, anticompetitive injunctions have imposed extraordinary burdens on iControl. For more than six months, Fintech has, with increasing success, used the threat of a sweeping injunction to pressure iControl's customers—including some that were never Fintech customers—to switch to Fintech. The prospect that the Court might enter such an injunction has also made it difficult for iControl to secure necessary financing from its investors and lenders, including to fund a supersedeas bond to enable iControl to appeal the judgment in this case. iControl respectfully requests that the Court lift these unfair burdens once and for all by denying Fintech's renewed motion with prejudice.

ARGUMENT

I. The Court should deny Fintech's renewed motion as untimely.

Fintech has not established that its untimely filing was due to "excusable neglect." Fed. R. Civ. P. 6(b)(1)(B). "'Excusable neglect' is not easily demonstrated, nor was it intended to be." *Thompson v. E.I. DuPont de Nemours & Co.*, 76 F.3d 530, 534 (4th Cir. 1996). Courts consider the following factors as bearing on excusable neglect: "(1) the danger of prejudice to the nonmovant; (2) the length of the delay and the impact on judicial proceedings; (3) the reason for the delay, including whether it was within the reasonable control of the movant; and (4) whether the movant acted in good faith." *Zurich Am. Ins. Co. v. Euro. Tile & Floors, Inc.*, 2017 WL 638640, at *2 (M.D. Fla. Feb. 16, 2017). Here, those factors weigh decisively against Fintech.

First, Fintech's delay is highly prejudicial to iControl. iControl reasonably assumed that Fintech's failure to file on the deadline set by the Court reflected a deliberate strategic decision not to seek a narrower injunction. In reliance on Fintech's apparent decision, iControl participated in good faith in settlement negotiations with Fintech with the understanding that there would be no injunction in this case. Only after iControl pointed out, in the course of those settlement discussions, that Fintech had lost negotiating leverage by not renewing its injunction motion did Fintech seek permission to late-file. iControl also relied on Fintech's failure to file in extensive discussions and negotiations with iControl's investors. Those delicate negotiations have now been thrown into turmoil by Fintech's attempt to revive the injunction issue that iControl reasonably believed was off the table. iControl is a much smaller company than Fintech and has struggled to survive Fintech's attacks—both those in court that led to a damages judgment that iControl is attempting to bond and those outside of court designed to scare iControl's customers into switching to Fintech even absent an injunction. iControl was entitled to rely on this Court's clear deadline and on Fintech's failure to meet that deadline, and it should not be penalized for having done so.

Second, judicial efficiency would not be served by entertaining Fintech's belated second injunction motion. Fintech has already gained nearly six months of commercial advantage from its original, overly broad injunction motion. Fintech could have sought a narrower injunction in its original motion or in a timely renewed motion. Allowing Fintech a third bite at the apple would not promote efficiency or respect for the judicial process. Moreover, while Fintech's delay was "only" three days, it would no doubt have been much longer had iControl not alerted Fintech to the deadline in the course of good-faith settlement negotiations.

Third, Fintech's reasons for the delay do not warrant relief. The August 17 deadline was set out in bold in the conclusion of this Court's four-page order, in the same sentence that required Fintech to identify its trade secrets "with reasonable specificity." Doc. 279 at 4. Fintech says it missed the deadline because counsel "inadvertently failed to calendar" it, Doc. 284 at 2, but this is a red herring. The deadline was not for some remote task that counsel would turn to weeks or months in the future; the renewed motion was due just *seven days later*. With the deadline so close at hand, counsel hardly needed to "calendar" it to keep it in mind. The real issue is counsel's failure to *read* the Court's order, or at least to read it carefully enough to notice the deadline. Fintech has multiple lawyers on this case. It has provided a declaration from only *one* of those lawyers—Ms. Molloy, who states that she "read the order completely and must have seen" the deadline but failed to "recognize" that it was seven days away. Doc. 284-2 at 2. But the Court's order was also served on Mr. McCrea, a partner at Greenberg Traurig. Mr. McCrea has not provided any declaration, and Fintech has not represented that Mr. McCrea read the Court's order *at all*.

"[I]t is well settled that failure to read or comprehend a court order will not satisfy the excusable neglect standard." *Batista v. City of N.Y.*, 2007 WL 2822211, at *6 n.3 (S.D.N.Y. Sept. 25, 2007); *accord In re A.A. & Assocs., Inc.*, 2009 WL 2447608, at *2 (W.D. Ky. Aug. 7, 2009)

("[T]he failure to read and comprehend the plain language of a court's order can never constitute excusable neglect."). As Judge Kovachevich in this District has written, it would be "preposterous" to treat an attorney's failure to read an order as excusable neglect: "To allow an attorney to simply claim that he or she was unaware of a court order, simply for the attorney's failure to read the court's order, is not only nonsensical, it fails to comport with notions of adequate representation, something this Court will not stand for." *Robinson v. Aerotek, Inc.*, 2011 WL 2222186, at *2 (M.D. Fla. June 7, 2011); *see also Freeman v. Rice*, 2012 WL 12949620, at *2 (S.D. Fla. Apr. 25, 2012) ("It is axiomatic that attorneys of record are required to read all court orders in their entirety.").[1]

For that matter, even "[c]alendaring errors" generally do not qualify as excusable neglect. *Rayford v. Karl Storz Endoscopy Am., Inc.*, 740 F. App'x 435, 437 (5th Cir. 2018). Courts in this District and elsewhere routinely hold that a mere "failure to correctly calendar the deadline to file a motion … , absent more, is not excusable neglect." *Wright v. Dyck-O'Neal, Inc.*, 2016 WL 3912050, at *5 (M.D. Fla. June 27, 2016).[2] But that is beside the point. The missed deadline here

[1] Decisions so holding are too numerous to count. *See, e.g.*, *Two-Way Media LLC v. AT&T, Inc.*, 782 F.3d 1311, 1317 (Fed. Cir. 2015) (no abuse of discretion in concluding "it was inexcusable for AT&T's multiple counsel to fail to read all of the underlying orders they received"); *Williams v. Va., State Bd. of Elections*, 524 F. App'x 40, 41-42 (4th Cir. 2013) (no abuse of discretion in denying relief based on "counsel's admission that she inadvertently failed to read the court's … order"); *Gonzalez v. Cty. of L.A.*, 2020 WL 2797282, at *3 (C.D. Cal. May 29, 2020) ("Failing to read the Court's Order and recognize that certain claims were dismissed with prejudice is not excusable neglect, it is clear carelessness."); *Corsair Special Situations Fund, L.P. v. Engineered Framing Sys. Inc.*, 2013 WL 6773570, at *5 (D. Conn. Dec. 19, 2013) ("Attorney Zeitlin's failure to read and appreciate the significance of the court's Notice to Counsel and Order is not excusable."); *Hicks v. Transit Mgmt. of Asheville, Inc.*, 2012 WL 1313217, at *3 (W.D.N.C. Apr. 17, 2012) ("Counsel's neglect in failing to read an Order of the Court and to comply with its directives" is not excusable neglect); *Zivanic v. Wash. Mut. Bank, N.A.*, 2010 WL 4975558, at *1 (N.D. Cal. Dec. 2, 2010) (counsel's "failure to read the concluding lines of the Court's order … does not constitute excusable neglect").

[2] *See also, e.g.*, *Zurich*, 2017 WL 638640, at *3 ("overlooking deadlines" is "within the movant's control and do[es] not constitute excusable neglect"); *Puerto v. Moreno*, 2020 WL 2308480, at *2 (S.D. Fla. May 8, 2020) ("the inadvertent failure to calendar the motion deadline

resulted not from a calendaring error but from a failure, by multiple lawyers, to read and comprehend the Court's straightforward order. None of the cases Fintech cites involved a failure by multiple attorneys to read an order setting forth a clear deadline that was just seven days away. And as the cases cited above make clear, such a failure can *never* constitute excusable neglect.

Fourth, and relatedly, "good faith is not found where the party is merely ignorant of a court's rules and deadlines." *Zurich*, 2017 WL 638640, at *3. And good faith alone "does not warrant a finding of excusable neglect." *Melgar v. M.I. Quality Lawn Maintenance, Inc.*, 2010 WL 11553187, at *2 (S.D. Fla. Dec. 8, 2010). For example, this Court held that the United States' failure to timely appeal due to "the mistake of counsel in failing to calendar properly the deadline" was not excusable even though "[n]either party dispute[d] the United States' good faith." *In re Lykes Bros. Steamship Co.*, 2009 WL 3157630, at *2 (M.D. Fla. Sept. 28, 2009) (Merryday, J.).

"A deadline is a deadline. It is not a suggestion …." *EEOC v. Joe Ryan Enters., Inc.*, 2013 WL 499892, at *3 (M.D. Ala. Feb. 8, 2013). iControl was entitled to rely on the clear deadline this Court set, and it did so. iControl asks the Court to enforce that deadline.

II. The Court should also deny Fintech's renewed motion on the merits.

A. Legal Standards

A permanent injunction is "a drastic and extraordinary remedy," *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 165 (2010), that "does not follow from success on the merits as a matter of course," *Winter v. NRDC, Inc.*, 555 U.S. 7, 32 (2008). When an injunction is warranted, it must be "narrowly tailored to fit the specific legal violations adjudged" and to "restrain no more than what is reasonably required to accomplish its ends." *Keener v. Convergys Corp.*, 342 F.3d 1264,

… was not excusable neglect"); *Sream, Inc. v. Ecstasy Fashion II, Inc.*, 2018 WL 10374693, at *2 (S.D. Fla. Sept. 19, 2018) (no excusable neglect where plaintiffs "provided no other reason" for their untimely filing "apart from their system's failure to calendar the requisite deadlines").

1269 (11th Cir. 2003) (internal quotation marks omitted). In a trade-secrets case, the scope of any injunction must "be carefully framed to avoid undue restraint on legitimate competition." Restatement (Third) of Unfair Competition § 44 (2020). That is why, as this Court has held, any injunction here must be limited to *specific* trade secrets found to have been misappropriated.

Moreover, it is "impossible to tell from the general verdict" in this case (Doc. 245 at 1) which of the alleged trade secrets the jury found were protected and had been misappropriated. *United States v. An Article of Drug*, 661 F.2d 742, 746-47 (9th Cir. 1981). So if the Court chooses to enter an injunction, it must "determine[] the scope of the injunction based upon [its own] view of the facts established by the evidence." *Id.* Although the Court determined that a "reasonable juror could [have found] that iControl misappropriated Fintech's trade secrets," Doc. 279 at 2, the Court did not make any findings as to *which* of the alleged trade secrets (1) are in fact protectible as trade secrets and (2) were misappropriated by iControl. In order to enter an injunction, the Court must make specific findings on those points; it cannot simply rely on the verdict. *See McCarthy v. Fuller*, 810 F.3d 456, 460-61 (7th Cir. 2015) (where general verdict found defendants had defamed plaintiffs but "didn't indicate specifically which [statements] it found to be defamatory and to have been made by the defendants, the judge had no basis in the jury's verdict for issuing an injunction" and had to "mak[e] his own factual determinations" to justify any injunction); *N. Ind. Gun & Outdoor Shows, Inc. v. Hedman*, 104 F. Supp. 2d 1009, 1011 (N.D. Ind. 2000) (where court could not "say with confidence what findings the jury made to reach" its general verdict, court made its own factual findings and concluded no permanent injunction was warranted).

If the Court does make findings justifying the entry of an injunction, the injunction must "state its terms specifically" and "describe in reasonable detail … the acts or acts restrained or required." Fed. R. Civ. P. 65(d)(1). "[A]n ordinary person reading the court's order should be able

to ascertain from the document itself exactly what conduct is proscribed." *Hughey v. JMS Dev. Corp.*, 78 F.3d 1523, 1531 (11th Cir. 1996) (quotation omitted). The Rule seeks to eliminate "one of the principal abuses of the pre-federal rules practice—the entry of injunctions that were so vague that defendant was at a loss to determine what he had been restrained from doing." *Id.* (quotation omitted). Subjecting iControl to the possibility of a contempt citation based on an "insufficiently specific injunction" would violate not only Rule 65, but also due process. *LabMD, Inc. v. FTC*, 894 F.3d 1221, 1235 (11th Cir. 2018).

B. The top-level terms of the proposed injunction are wildly overbroad.

At the highest level, the proposed injunction would prohibit iControl from disclosing or making use of either "Fintech's regulated commerce software system" or "iControl's Harmony software, as modified, for the regulated commerce industry." both of which it characterizes as "trade secret information belonging to Fintech." Doc. 284-1 at 8-10. It also purports to identify more "specific trade secrets" that are "includ[ed]" within these broad prohibitions, *id.* at 8-9, but it does not *limit* the scope of the proposed injunction to those supposedly "specific" trade secrets.

Such sweeping prohibitions have no basis in law. Countless elements of Fintech's "regulated commerce software system" are not trade secrets by any stretch of the imagination. It is well established that "outward-facing features that every user of [a software program] can see and experience are not trade secrets." *Calendar Research LLC v. StubHub, Inc.*, 2018 WL 4846797, at *4 (C.D. Cal. Aug. 7, 2018); *see IDX Sys. Corp. v. Epic Sys. Corp.*, 285 F.3d 581, 584 (7th Cir. 2002); *Warehouse Sols., Inc. v. Integrated Logistics, LLC*, 2014 WL 12647878, at *6 (N.D. Ga. July 7, 2014), *aff'd*, 610 F. App'x 881 (11th Cir. 2015). And Fintech is not even content to claim *its own* software system as a trade secret; it also claims that *iControl*'s software is, in its entirety, "trade secret information belonging to Fintech," Doc. 284-1 at 8, 10, because when iControl "modified its existing Harmony software for the regulated commerce industry," Fintech's

"trade secrets were incorporated into iControl's Harmony software." Doc. 284 at 14. This echoes Fintech's original injunction motion, which argued that "it would not be enough merely to prohibit iControl from using Fintech's trade secrets" because "iControl's entry into the regulated commerce business was premised on its misappropriation of Fintech's trade secrets." Doc. 249 at 5. But the Court *rejected* that argument and ordered Fintech to identify "with reasonable particularity the *specific* trade secrets" at issue. Doc. 279 at 4 (emphasis added).

Mapei Corp. v. J.M. Field Marketing, Inc., 295 So. 3d 1193 (Fla. 4th DCA 2020), does not support Fintech. The court there held that J.M.'s "inventory management software program" enjoyed trade-secret protection because its features were "unique and not well-known or available in the market" and because J.M. "took reasonable measures to protect its trade secrets from the general public and competitors," including requiring potential clients to sign a confidentiality agreement before they could even see a demonstration of the software. *Id.* at 1195, 1198-99. Even so, the court did not hold that the parties accused of misappropriating J.M.'s trade secrets could be enjoined from using their own competing software. Rather, it held that J.M. was entitled to a temporary injunction "against ongoing and continued use of its trade secrets," and it remanded for the trial court to fashion an appropriately tailored injunction. *Id.* at 1201.

This case is nothing like *Mapei*. Fintech has not shown that the outward-facing features of its software were "unique and not well-known" or that it took appropriate steps to preserve their confidentiality. *Id.* at 1198. Just the opposite. As explained below, the features Fintech claims as trade secrets are elementary and widely practiced. Moreover, Fintech disclosed the existence of these features to actual and potential customers, third-party banks, and the general public without any confidentiality restrictions. So it is Fintech's burden to identify with particularity which aspects of its system are trade secrets. It has not done so. And if it had, that would entitle it only

to an injunction against continuing use of whatever *specific, identifiable* trade secrets the Court finds (1) are legally protectible and (2) were misappropriated by iControl.

C. The supposedly more "specific" terms of the proposed injunction fail to identify Fintech's protectible trade secrets with reasonable particularity.

Paragraphs I(A)(1)–(5) of the proposed injunction purport to identify more "specific" trade secrets for which Fintech is seeking protection. Doc. 284-1 at 8-10. But these paragraphs do not identify the trade secrets with reasonable particularity. Instead, they are so broad and vague that they (1) encompass information that is not protectible as a matter of law, and (2) would leave iControl at a loss about what the injunction prohibits. We address each paragraph in turn.

1. Fintech's "Invoice Process"

First, in paragraph 1(A)(1), Fintech asks the Court to enjoin iControl from using:

> 1. Fintech's invoice process in the regulated commerce industry, including:
>   a. The database architecture and data structure of Fintech's invoices, including the invoice header, detail, and mandatory use of the vendor item number, and the structure and maintenance of service adjustment, promotion, and charge ("SAC") codes;
>   b. Fintech's exception rules, including the logic coded into Fintech's system to verify the fields on the invoice; and
>   c. Fintech's in-system editor.

Doc. 284-1 at 8-9. The general prohibition on using "Fintech's invoice process" is plainly overbroad. Fintech has never claimed that *every* aspect of its "invoice process" is a trade secret. And the word "including" suggests that iControl would be prohibited from using other, unspecified aspects of Fintech's invoice process, not limited to the items described in subparagraphs (a), (b), and (c). iControl has no idea what those other aspects might be, and the proposed injunction does not provide any guidance. And the subparagraphs are no better:

a. "Database Architecture." It is not clear what Fintech means by the "database architecture and data structure of Fintech's invoices." While the term "database architecture"

might seem to relate to how Fintech stored data within its computer systems, Fintech's expert, Mr. Zatkovich, never purported to describe the organizational structure of Fintech's internal computer databases. 2/26 Tr. 182:1-19. Instead, he appeared to equate "database architecture" with the way Fintech organized its standard distributor invoice. But the organization of Fintech's invoices cannot possibly be a trade secret. While Fintech's internal computer architecture might have been secret, its invoices were visible to tens of thousands of Fintech's customers and their third-party agents, *see* 2/26 Tr. 55:3-10, as well as to anyone who watched the video demonstration on Fintech's website, *see* Def.'s Ex. 254. And if there is something specific about Fintech's invoices that might qualify as a trade secret, the proposed injunction gives no hint about what it might be.

The vague reference to "invoice header" and "detail" only confuses matters further. Mr. Zatkovich testified that Fintech's invoices include a "header" with "all the main information" (*e.g.*, invoice number and customer name) followed by a "detail" section with line items for individual products. 2/26 Tr. 54:16-55:6. But he never claimed this was a trade secret. That would have been absurd: Anyone who has ever seen an invoice for almost any type of product or service—say, a utility bill or a restaurant check—is familiar with this basic way of organizing an invoice. Does the proposed injunction mean that iControl's invoices cannot include "header" and "detail" sections *at all*? Or does it mean only that iControl cannot use headers and details in *some specific way* that would be similar to how Fintech uses them? If so, how would iControl have to redesign its invoices to avoid the risk of contempt? The proposed injunction does not say.

Equally confusing is the reference to "the structure and maintenance of service adjustment, promotion, and charge ('SAC') codes." SAC codes are not something Fintech invented—they are required by customers and are a basic feature of processing payments in any industry. *See, e.g.*, *id.* at 56:15-57:4; 2/28 Tr. 53:2-13; *see also, e.g.*, EDI Academy, *X12 Allowance and Charge Codes*,

https://bit.ly/3lIQccL (explaining SAC codes and providing examples). Mr. Zatkovich never claimed that processing SAC codes is a trade secret. Rather, he testified that Fintech had "developed a specific database structure to maintain this information." 2/26 Tr. 57:5-10. But he never described specifically what is unique about the way Fintech handles SAC codes; nor does the proposed injunction. iControl does not know what Fintech is claiming as its proprietary method of processing SAC codes, and it is not clear whether the proposed injunction would require iControl to make any changes in the way it currently handles SAC codes.[3]

b. "Exception Rules." Nor is it clear what it would mean for iControl to be prohibited from using "Fintech's exception rules." Exception rules in general are not a trade secret; they are just simple rules to detect errors or missing information on an invoice. For example: (1) Confirm that the invoice number is included. (2) Confirm that the supplier name is included. (3) Confirm that the item description is included. (4) Make sure the invoice date is in the past, not the future. Rules like these are a basic feature of any payment-processing software. They will be familiar to anyone has ever performed any kind of digital transaction (such as a purchase on Amazon.com) and been notified of some missing information (like a credit card expiration date). Fintech cannot seriously contend that such basic, widely used rules are its proprietary trade secrets. Perhaps that is why the proposed injunction does not say iControl cannot use *any* exception rules, just that it cannot use *Fintech's* exception rules. But Fintech has never identified its supposedly unique exception rules, and iControl therefore has no way of knowing whether it is using "Fintech's" rules.

[3] By contrast, iControl *thinks* it understands what Fintech means by "mandatory use of the vendor item number." Mr. Zatkovich testified that Fintech uses "vendor identification numbers," (VINs) as a "master index" to identify products and requires its customers to supply them. 2/26 Tr. 55:22-56:4. iControl does not agree that this is a trade secret. Regardless, it is undisputed that iControl does not use VINs as a "master index" or require its customers to provide VINs; it merely gives them the option of doing so. *See* 2/28 Tr. 55:12-18; *id.* at 184:7-22. iControl would be willing to stipulate that going forward, it will continue not to require its customers to provide VINs.

c. "In-System Editor." It is also not clear what the proposed injunction means by prohibiting iControl from using "Fintech's in-system editor." Mr. Zatkovich testified that when an invoice is found to contain errors or omissions, Fintech's software does not "kick back the invoice" but instead allows the customer to access an "in-system editor" to fix the errors. 2/26 Tr. 60:14-61:15. But the fact that Fintech's software had this capability was not a trade secret; it was something that all of Fintech's customers knew about. This is also a common feature in other payment-processing software. *See, e.g.*, Wave Help Center, *How To View, Edit, or Delete an Invoice*, https://bit.ly/32I7DBG; Recurly, *Edit Invoice*, https://bit.ly/3hMhlJA. Mr. Zatkovich did not identify any secret, proprietary process relating to *how* Fintech provides its invoice-editing feature. Neither does the proposed injunction. Would Fintech argue that the proposed injunction requires iControl to prevent customers from editing their invoices *at all*? Is it enough that iControl does in fact "kick back" invoices found to contain errors, and that in-system editing is available only for invoices *not* found to contain errors? Is there some other aspect of Fintech's editing feature that iControl would have to avoid duplicating? The proposed injunction does not say.

2. Fintech's "Payment Process"

Next, in paragraph I(A)(2), Fintech asks the Court to enjoin iControl from using:

> 2. Fintech's payment process in the regulated commerce industry, including:
> a. The extraction of information from the invoices and calculation and aggregation of the invoices for processing in one daily ACH transaction; and
> b. The use of debit filters or "white filters."

Doc. 284-1 at 9. The general reference to Fintech's "payment process," like the general reference to Fintech's "invoice process" in paragraph I(A)(1), is plainly overbroad. Fintech has never claimed that *every* aspect of its "payment process" is a protected trade secret. Nor do the two subparagraphs clear things up:

a. "Extraction," "Calculation," and "Aggregation." What the proposed injunction means by "extraction of information from the invoices" is anyone's guess. Mr. Zatkovich never testified about any trade secrets involved in "extracting" information from invoices. He did refer briefly to "[l]ots of individual adjustment code[s] that have to be calculated, make sure that they're pulled, processed, calculated, taxes, delivery fees, split cases." 2/26 Tr. 68:11-13. But he did *not* assert that the process vaguely described in that single run-on sentence involved any trade secrets, much less attempt to explain what those trade secrets might be. Would the proposed injunction require iControl to stop "extract[ing]" information from invoices altogether—which would mean not processing payments at all? Or would iControl only have to stop using specific *methods* of extraction claimed as proprietary by Fintech? If so, what are those methods?

The reference to "calculation and aggregation of the invoices for processing in one daily ACH transaction" is also unclear. Needless to say, processing payments based on invoices always involves *some* "calculation." Presumably Fintech is not asking the court to forbid iControl from doing math. But then what *is* Fintech saying? The aspect of Fintech's "calculations" that received the most attention in Fintech's trial presentation was the "rounding" of decimal numbers. But the proposed injunction does not mention rounding—presumably because at trial, it was undisputed that iControl does *not* use the same rounding method as Fintech. *See* 2/28 Tr. 189:11-190:9. Moreover, aggregating multiple invoices into a single transaction cannot possibly be a trade secret. Aggregating transactions is a basic element of financial life, just as millions of businesses combine the day's receipts into a single bank deposit at day's end. And Fintech's use of aggregation was not a secret—it was known to the third-party banks, who were free to share that information with others. Fintech cannot seriously be claiming that no one but Fintech should be allowed to aggregate multiple invoices into one transaction. And if Fintech is claiming it has some secret, proprietary

method of aggregating invoices (other than simple addition), the proposed injunction does not describe that method or give iControl any way of knowing whether it is using Fintech's method.

b. "Debit Filters or 'White Filters.'" Even Mr. Zatkovich never claimed that "debit filters" were a trade secret. On the contrary, he explained that banks routinely use "debit filters" to identify and block suspicious transactions, noting that "everybody's experienced debit filters with their credit card." 2/26 Tr. 71:7-8; *see id.* at 86:11-12. There is accordingly no basis for enjoining iControl and its partner banks from using debit filters. What Mr. Zatkovich *did* claim as a trade secret were what he called "white filters." He testified that Fintech "work[ed] with the banks" to let them "know … the distributors associated with each customer at each bank account" so that the banks could "maintain that information as a white filter … for the sole purpose[] of making sure that transaction does not get blocked." *Id.* at 72:5-12. But Fintech could not, and did not, keep the existence of "white filters" to itself. The banks that worked with Fintech to implement the white filters necessarily knew about them, and nothing stopped those banks from providing the same service to iControl. Mr. Zatkovich admitted that banks like Fifth Third are "involved in" the process of setting up white filters and that iControl could have learned about white filters from its banks. *Id.* at 191:19-192:11; *accord* 2/28 Tr. 227:5-8 (Dr. Malek testifying that debit filters and white filters are "not a trade secret of Fintech" but "a feature provided by banks" to their clients). The proposed injunction does not identify any secret, proprietary *method* that Fintech used to implement white filters; it just claims *any* use of white filters as a trade secret, despite the banks' knowledge and involvement. That position is untenable.

It is not even clear what Fintech would consider a "white filter." Mr. Zatkovich provided only a general description of the concept. If a bank requests information from iControl, which the bank then uses to avoid inappropriately blocking transactions, would that violate the proposed

injunction? Would Fintech argue that iControl must insist that its partner banks not make *any* efforts to avoid mistakenly blocking transactions—even efforts the banks would make in the ordinary course of their own business to avoid creating difficulties for their own customers? That would be absurd. But if the proposed injunction has some narrower meaning, iControl is at a loss to understand what it is.

3. Fintech's "Customer Specific" Interfaces

Next, in paragraph I(A)(3), Fintech asks the Court to enjoin iControl from using:

> 3. Fintech's customer specific and payment reconciliation interfaces, including:
> a. Fintech's FMS customer interface;
> b. Fintech's 820 interface for Houston Distributing; and
> c. Fintech's Starbucks interface.

Doc. 284-1 at 9. It is not clear what supposed "trade secret" this language is meant to protect. What Fintech misleadingly calls its "customer-specific interfaces" are in fact *the customers' property*, not Fintech's. "Customer-specific interfaces" is just a fancy way of saying that both Fintech and iControl have to use their customers' predetermined file formats. As Dr. Malek explained, each customer "already has a format they use for accepting … payments," and "if you are a third-party payment processing company, such as Fintech or iControl, you are going to have to abide by the file format that [the customers] require." 2/28 Tr. 190:15-191:12. Mr. Zatkovich acknowledged that a customer "is going to dictate to folks like iControl what fields they require to communicate with [the customer's] system." 2/26 Tr. 193:18-21. Many customers even post their file format specifications on the Internet for vendors to use. 2/28 Tr. 50:10-23.

Fintech's proposed injunction would prohibit iControl from using "*Fintech's* FMS customer interface," "*Fintech's* 820 interface for Houston Distributing," and "*Fintech's* Starbucks interface" (emphases added). But these "interfaces" belong to *the customers*, not to Fintech. It is undisputed that Homeland Foods, Houston Distributing, and Starbucks sent iControl the

information necessary to interface with their accounting systems. 2/26 Tr. 95:10-11, 96:3-10, 97:12-21, 98:5-23. In fact, when Fintech objected to Starbucks sharing this information with iControl, Starbucks responded with incredulity: It explained that the information pertained to "Starbucks standard formats" that "all [of Starbucks'] suppliers" were required to use. Pl.'s Ex. 94F at 2. And Fintech even conceded the point: It said it did not object to Starbucks' sharing the customer-specific file format that Fintech had "[d]eveloped with" Starbucks. *Id.* So it is not clear what Fintech means when it seeks to enjoin iControl from using "Fintech's customer specific … interfaces" or what iControl would have to do to interface with its customers without running the risk of being accused by Fintech of violating the injunction.

4. Fintech's Analytic Reports

Paragraph I(A)(4) of the proposed injunction would prohibit iControl from using:

> 4. Fintech's method and process to develop certain reports, including:
>   a. Fintech's method for developing and including information in its broken case report; and
>   b. Fintech's method for developing and including information in its price discrepancy report.

Doc. 284-1 at 9. This language appears purposefully vague. This Court has already held that Fintech's broken case and price discrepancy reports, which Fintech disclosed to its customers and to the public at large (*see, e.g.*, 2/26 Tr. 101:9-10), are not trade secrets. Doc. 211 at 5. The Court explained that neither "the source data for the report[s]," nor "[t]he contents" of the reports, nor "[t]he format in which the data is ultimately presented" in the reports could be a trade secret. 2/26 Tr. 120:25-121:17. The Court left open the possibility that "[t]he method by which the [underlying] data is arrayed … and manipulated" "in the hands of" Fintech might be a trade secret. *Id.* at 121:3-4. But Fintech has never attempted to describe any such secret, proprietary "method." As Dr. Malek pointed out at trial, Mr. Zatkovich "never showed us these methods. … [H]e talks about a

method, but then he shows a screen shot" of a finished report. 2/28 Tr. 193:6-12. Fintech employs the same tactics in the proposed injunction: It tries to circumvent this Court's ruling by referring vaguely to its "method" for creating broken case and price discrepancy reports. But iControl cannot ensure that it is not using Fintech's protected "method" if it does not know what that method is. For the same reasons, the Court should reject Paragraph I(C) of the proposed injunction, which would enjoin use of iControl's "Next Gen Reconciliation software to the extent it includes broken case and price discrepancy reports" without even the pretense of being limited to some proprietary "method." Doc. 284-1 at 10.

5. Fintech's "User Portal"

Finally, paragraph I(A)(5) of the proposed injunction would prohibit iControl from using:

> 5. Fintech's user portal and user interface model, including:
> a. Fintech's user portal functions; and
> b. Fintech's access model for its user portal.

Doc. 284-1 at 9-10. Like the rest of the proposed injunction, this paragraph neither identifies Fintech's protectible trade secrets with particularity nor gives iControl reasonable notice of what conduct is prohibited.

a. "User Portal Functions." It is not clear what the proposed injunction means by Fintech's "user portal functions." At trial, Mr. Zatkovich did not identify any specific, proprietary "functions" available in Fintech's user portal. Instead, he appeared to claim that *all* the "menus" and "functions" available in that portal, no matter how basic or essential, were trade secrets. 2/26 Tr. 129:14-17. This would be like Microsoft claiming that all the "menus" and "functions" in Microsoft Word are trade secrets, and therefore no competitor can create word-processing software with an "Edit" menu or a "Save" function. The menus and functions that were available to customers through Fintech's user portal were not trade secrets, because they were "details that ordinary users of the software could observe without reverse engineering," *IDX Sys.*, 285 F.3d at

584, and that Fintech made available to the public through a video demonstration on its website, Def.'s Ex. 254; *see* 2/28 Tr. 194:5-195:21. Moreover, since many of the "functions" that are available in Fintech's user portal are necessary to processing payments, a sweeping prohibition on iControl's offering similar "functions" would effectively bar iControl from competing with Fintech at all—a result this Court has already rejected. And if there are some *specific* "user portal functions" that Fintech claims as trade secrets, the proposed injunction does not identify them.

b. "Access Model." It is not clear what the proposed injunction means by "Fintech's access model." The evidence at trial made clear that Fintech does not have any secret, proprietary "access model" and, in any event, that iControl and Fintech regulate user access in fundamentally different ways. Fintech uses a "basic access control model" that requires a customer to determine the level of access for "each individual user"—a "very common" approach familiar to anybody with an "undergraduate degree in computer science." 2/28 Tr. 196:19-197:23. iControl uses a "more advanced, more sophisticated" approach known as "role-based access control," which allows a customer to assign each user a role (such as "store manager, regional manager, cashier," and so on) and then specify the level of access permitted for *all* users with that role. *Id.* at 197:24-198:22. Accordingly, there is no basis for enjoining iControl from using "Fintech's access model." And if the Court were inclined to enter such an injunction, it should make clear that the injunction applies only to a basic model where access rights are controlled for each individual user—the model employed by Fintech—and does not extend to iControl's more sophisticated system of controlling access rights based on users' roles.

D. Fintech has failed to justify the temporal sweep of the proposed injunction.

Even if Fintech had identified any trade secrets with reasonable particularity, it still would not be entitled to an injunction *five years* after the alleged misappropriation, much less a *perpetual* injunction. An injunction in a trade-secrets case must be limited to "the period of time it would

have taken" the defendant, "either by reverse engineering or by independent development, to develop its [product] legitimately without use of" the trade secrets. *K-2 Ski Co. v. Head Ski Co.*, 506 F.2d 471, 474 (9th Cir. 1974); *see also Concept, Inc. v. Thermotemp, Inc.*, 553 So. 2d 1325, 1328 (Fla. 2d DCA 1989) (citing *K-2* with approval). Mr. Zatkovich admitted that "[g]iven time," iControl "certainly" could have developed on its own "the specific functionality that [he] described … as FinTech's proprietary information and software." 2/26 Tr. 163:20-164:1. And iControl was not starting from scratch: It had been using "extremely sophisticated" software to provide non-alcohol payment services to "tens of thousands" of stores since 2005. 2/27 Tr. 90:13-19, 94:14-20, 105:18-24. To process alcohol payments, iControl merely had to make some adjustments to its existing platform; it did not have to create an entirely new platform, as "the underlying capabilities were … almost entirely the same." *Id.* at 105:25-106:18; *see also* 2/25 Tr. 116:3-5, 140:18-141:9. Given that the alleged misappropriation took place more than five years ago, iControl certainly could have developed the features in question independently by now, so no injunction is warranted. If the Court disagrees, it should limit the duration of any injunction to the period the Court determines it would have taken iControl to develop whatever protectible software features the Court finds iControl misappropriated. Moreover, any injunction should provide a reasonable period of time for iControl to come into compliance, in order to avoid the severe burdens on iControl's customers that would result if iControl were forced to suddenly terminate its regulated commerce business.

CONCLUSION

The Court should deny the renewed motion.

/s/ Jeffrey S. Bucholtz
Jeffrey S. Bucholtz (*Pro Hac Vice*)
Email: jbucholtz@kslaw.com
Paul Alessio Mezzina (*Pro Hac Vice*)
Email: pmezzina@kslaw.com
KING & SPALDING LLP
1700 Pennsylvania Ave. NW, Suite 200
Washington, D.C. 20006
Phone: 202-626-2907

Jonathan B. Sbar, Esq. (FBN 131016)
Email: jsbar@rmslegal.com
Robert L. Rocke, Esq. (FBN 710342)
Email: rrocke@rmslegal.com
Andrea K. Holder, Esq. (FBN 104756)
Email: aholder@rmslegal.com
ROCKE, McLEAN & SBAR, P.A.
2309 S. MacDill Avenue
Tampa, FL 33629
Phone: 813-769-5600

Attorneys for Defendant

CERTIFICATE OF SERVICE

I certify that on September 4, 2020, I electronically filed the foregoing via the Court's CM/ECF filing system, which will send a notice of filing to all counsel of record.

/s/ Jeffrey S. Bucholtz
Jeffrey S. Bucholtz (*Pro Hac Vice*)