SCHERER DESIGN GROUP, LLC, *Plaintiff,* - vs. - CHAD SCHWARTZ; AHEAD ENGINEERING LLC; FAR FIELD TELECOM LLC; KYLE McGINLEY, DANIEL HERNANDEZ *and* RYAN WALDRON, *Defendants*.	SUPERIOR COURT OF NEW JERSEY HUNTERDON COUNTY : CHANCERY DIVISION CIVIL ACTION NO.

MEMORANDUM OF LAW IN SUPPORT OF TEMPORARY RESTRAINING ORDER AND PRELIMINARY INJUNCTION

MANDELBAUM SALSBURG P.C.
Ronald D. Coleman
3 Becker Farm Road
Roseland, NJ 07068
973-736-4600
rcoleman@lawfirm.ms
Attorneys for Plaintiff
Scherer Design Group, LLC

PRELIMINARY STATEMENT

This case involves the theft, by management level employees, of trade secrets – proprietary engineering specifications, customer data, customized computer programming – as well as solicitation by those employees, along with a recently-departed former employee, of the valuable clients and employees of plaintiff Scherer Design Group, LLC ("SDG"), a telecommunications engineering firm built on the know-how and reputation of two decades of experience. Not only did these faithless employees download, copy and transfer their employer's valuable data and provide it to a pair of competing firms: They set up those firms and began working for them – using the misappropriated data and client information – even as they collected salaries from their soon-to-be former employer and relied on its trust to ransack it electronically until the moment for them to depart was ripe.

As set forth in the Verified Complaint and accompanying certification by the plaintiff's IT manager, this conduct was confirmed by logging data left behind on the plaintiff's computer network and the computers provided by plaintiff for defendants' use. Routine inspection of those computers after the mass resignation of three of the four individual defendants also revealed that this conduct was coordinated and memorialized in a series of Facebook Messenger conversations left brazenly unsecured on a company-provided computer used by one of the defendants. These messages also reveals the extent to which the four conspirators solicited the plaintiff's clients, transferred the work to their new enterprise – literally going into covert business against their own employer, encouraged, induced and in concert with the first individual defendant and the new companies they established.

Little is more revealing of the equities or the facts of this case than the cocksure Facebook Messenger lecture given by the mastermind of the defendants' plot, defendant Chad

Schwartz, in the midst of this larceny, concerning the advantages of insisting on contractual assurances to protect defendants' new enterprises from disloyalty. Believing that he is teaching a legal lesson, Schwartz writes, "What if I take all [our] clients and start my own company doing the exact same thing? Would you want me to do that to you? Well, guess what. I wouldn't want you to do it to me, either. And, SDG is pretty sorry that they didn't lock me down too."

Schwartz and his confederates are the ones who should be sorry – if not for their callous consciences, for the fact that with or without formal agreements governing confidentiality and loyalty, their conduct runs right down the middle of New Jersey many prohibitions against taking an employer's proprietary data – and its clients and employees – to set up a competing company "doing the exact same thing." SDG's Verified Complaint seeks relief on a variety of legal theories, but this application for preliminary protection of what is left of its business is premised on its clear-cut entitlement to relief under the New Jersey Trade Secrets Act, breach of employee loyalty and tortious interference with contract and prospective economic advantage.

STATEMENT OF FACTS[1]

Plaintiff SDG is a consulting engineering firm offering full service site design to the telecommunications industry. Its team is made up of engineers, technicians, and inspectors with unique real-world practical experience in both design and inspection in a growing and increasingly important niche field of civil engineering, the design and engineering of antennas and antenna systems for wireless carriers and associated providers of wireless connectivity.

Defendant Chad Schwartz, a former employee of SDG, is the principal and president of defendants Ahead Engineering LLC ("Ahead Engineering") and Far Field Telecom LLC ("Far

1 A complete statement of the facts is set forth in the Verified Complaint filed in this action and is incorporated by reference herein. All the averments herein are based on the Verified Complaint and the Certification of Jason Gerstenfeld.

Field"), companies established by him shortly after his December 22, 2017 resignation from DSG along with the secret cooperation and planning of three SDG employees who remained with the company. Those three, defendants Daniel Hernandez, Kyle McGinley and Ryan Waldron, joined Schwartz at Ahead Engineering and Far Field after his departure – but only after they spent weeks downloading and copying SDG's proprietary data, technical specifications, client job details and other files, and helping Schwartz move several of SDG's most important clients to the competing business they set up.

The heart of SDG's proprietary design engineering system is an invaluable, proprietary relational database containing a wealth of information, available nowhere else in such a form or to such an extent, drawn from the 10,000 macro antenna, microcell, DAS and oDAS sites and site upgrades its founders and management have designed over 20 years. Broadly speaking, SDG's database consists of internal engineering test results, original survey data, published specifications and dozens of other critical data points relating to each of the 10,000 antenna projects its predecessors and staff have designed. As this information is collated and generated by SDG personnel in the field and over the course of project at a considerable investment of time and resources, it is digitized, converted to a form useable by SDG's proprietary engineering design system and collated by category.

SDG has also recently expanded successfully into development and sale of a range of designs and products related to antenna engineering and installation. One example of such products is systems for antenna concealment, a niche that has seen rapid growth as the explosion in the number of cell sites and oDAS installations comes up against increasing demands that to minimize or eliminate the aesthetic cost to the facilities and visual environments hosting them.

SDG's clients include wireless carriers, almost every one of which has engaged its services, as well as third-party vendors that contract with these carriers to provide turnkey antenna installations. A recent focus of SDG's business and its growth has been the design and data implementation for distributed antenna systems (DAS) and outdoor distributed antenna systems (oDAS) to service what are called outdoor distributed networks, which enable mobile connectivity and superior wireless service in urban, suburban and rural settings. oDAS installations are typically located on existing infrastructure such as utility telephone poles, street lamps or traffic signal poles, providing a high density of potential site candidates and makes them well-suited for areas that are otherwise difficult to serve, require coverage enhancements or require greater network capacity.

Much of SDG's DAS and oDAS recent work has been for ExteNet Systems, Inc., a leading provider of outdoor distributed networks ("ExteNet"). To service ExteNet's needs, SDG developed a proprietary system internally referred to as the "Extenet Automation," detailed below, that enables it to apply intimate knowledge of each aspect of site design, process and planning in a quantitative and rigorous manner, simultaneously generating all necessary construction documents, submissions for zoning and land use permitting and FAA documentation.

SDG'S Proprietary Site Database

The data generated and collated by SDG from over 20 years of experience include or reflect engineering and design experience informed by past telecommunications installations, including equipment installed, modifications or specifications relating to such installations based on testing and simulation by SDG with respect to local conditions such as wind, height, load, precipitation, temperature, moisture and other factors, applicable contractual, leasing and right-

of-way information affecting the legal status, costs for and access to such installations. SDG's database also includes a vast range of physical, construction, testing, technical, regulatory, safety-code and experience-based data that affect telecommunications antenna design. SDG also maintains valuable electronic engineering and design catalogs of site-based specifications and drawings with respect to all materials, configuration, aesthetic and other specifications utilized or required by each affected municipality and utility provider with respect to configurations and alternative tower structures or concealment protocols.

The database described above itself provides SDG with a considerable competitive advantage in its field because this vast amount of information does not have to be collected from innumerable sources when the same site requires upgrading or alteration. And it is particularly valuable at the present time because wireless providers are in a race to offer connectivity via new higher-speed wireless data protocols such as 5G which cannot be accommodated by existing antennas, requiring the installation or upgrading of antennas at sites for which permits and leases are needed. Developing a comparable database reflecting the range of factors set forth above for 10,000 antenna instillations comparable to that compiled and converted into accessible, usable form by SDG would be cost prohibitive for any new entrant into the markets in which SDG operates.

SDG's Proprietary Engineering Design System

What was becoming one of SDG's most important clients ExteNet, owns and operates multi-carrier, often referred to as "neutral-host", and multi-technology distributed networks that enable multiple wireless service providers to provide 3G and 4G service to mobile and other wireless users. ExteNet dominates the market for building out wireless broadband data in and around New York City, an area which SDG has long served and in which the demand for

wireless data is increasing at a phenomenal rate, resulting in tremendous strain on the existing wireless infrastructure serving the city.

Beginning in or around 2016, the demand from ExteNet for SDG's engineering services led SDG management's to recognize that most of ExteNet's installations involved relatively standardized solutions based on a definable range of configurations, regulatory parameters and other local factors. SDG invested resources into developing the ExteNet Automation system, a client-specific, automated system that could collate, catalog and employ this information and rapidly convert it to tested standardized models, processes and engineering approaches adapted to each new ExteNet installation. Part of the ExteNet Automation project, for example, SDG created a comprehensive design library containing drawings and specifications for every "pole appurtance" – accessories, structures attached to utility and lighting poles – in New York City.

SDG's ExteNet Automation collects, analyzes and integrates information such as this as well as from SDG's site databases, along with public sources such as the Internet, and then digitizes and converts it into the documentation ExteNet needs to obtain approvals from the FAA, New York City and each specific wireless provider. This process is performed by a suite of technologies coordinated on its Windows computers by customized code developed by SDG using the Visual Basic programming language, hypertext markup language (HTML) code, spreadsheets, CAD files which SDG engineers employ to produce experience-tested final designs with full sets of drawings and documentation.

SDG's investment in its ExteNet Automation program enabled it to produce fast-turnaround drawings and documentation to accommodate ExteNet's growing list of projects in and around New York City at a cost that reflected that efficiency over the course of 2017. By investing substantial financial and management resources, as well the know-how needed to direct

the organization of that data, SDG created a valuable proprietary conservatively worth millions of dollars. The competitive advantage provided by ExteNet Automation was significant, and SDG's investment was showing very significant returns. From 2016 to 2017, SDG's billings to ExteNet increased from approximately $43,000 to over $1.4 million, and was projected to grow to at least triple that amount, i.e., to well over $3 million.

Beginning in December of 2017, however the defendants ripped the ExteNet business away from SDG – from inside SDG itself. Conspiring to establish a rival firm, Ahead Engineering, while most of them were paid SDG employees, they wholesale transferred the data and programming SDG developed to serve ExteNet to their new company using their employee access to the SDG's computers and client relationships, right under the trusting nose of SDG.

Securing SDG's Proprietary Data and System

SDG's site information database and the ExteNet Automation were only accessible to authorized staff at SDG, and could only be accessed through SDG's secure Windows-based domain network and SDG-supplied and –configured computers. Only authorized SDG employee had access to SDG's computer network. The conspiracy among the defendants, therefore, depended on a plan led by defendant Chad Schwartz, a trusted SDG senior engineer who resigned in mid-December of 2017, pursuant to which defendants Daniel Hernandez, Kyle McGinley and Ryan Waldron would retain their jobs and salaries at SDG while assisting Schwartz in setting up two competing firms. Starting no later than late December and continuing until their own resignations from SDG on January 16, 2017, Hernandez, McGinley and Waldron were directed by Schwartz and other employees of Ahead Engineering and Far Field to systematically copy SDG computer files they anticipated using at their new firms until they were ready to resign *en masse* and compete with SDG using SDG's technology, data, clients.

Chad Schwartz's Resignation and the Conspiracy against SDG by its own Employees

The mastermind of this conspiracy, defendant Chad Schwartz, is a Professional Engineer with a degree in mechanical engineering who was hired by SDG's predecessor in 2000, rising to become a project manager and eventually Director of Engineering at SDG. Schwartz was closely involved in the development, maintenance, programming and application of the ExteNet Automation and development of valuable new products such as systems and designs for concealment of antenna installations. SDG reposed great trust in Schwartz, who had full access to every aspect of the ExteNet Automation system, the data on which it was based and was intimately involved in business and technical relations between ExteNet and SDG. And, in mid-2017, SDG approached Schwartz and presented him with the opportunity to become an equity partner in SDG on very generous terms.

During the course of negotiations, however, Schwartz expressed dissatisfaction with SDG's plans regarding the direction of SDG's short-term future growth, and relations between SDG's principals and Schwartz deteriorated through the fall of 2017. On November 27, 2017 Schwartz resigned from SDG effective December 22, 2017. Soon after his resignation, Schwartz agreed with defendants Hernandez, McGinley and Waldron to set up a pair of new engineering firms, defendants Ahead Engineering and Far Field to compete with SDG. Ahead Engineering describes itself on its LinkedIn profile as "a new, full-service telecom engineering firm composed of experienced telecom engineering professionals." Ahead Engineering, in fact, was established to compete with SDG's core business – with a particular focus on ExteNet. In contrast, the Internet profile of Far Field describes it as offering "innovative, cost effective solutions for oDAS and small cell site concealment." Far Field, in fact, was established to compete with the SDG antenna concealment products defendants had been paid to develop as

part of their work for SDG. Indeed, defendant Far Field wasted no time in offering and deploying proprietary SDG technology and processes for concealment lifted wholesale from SDG without authorization from or compensation to SDG.

Schwartz, in turn, undertook to formalize and monetize his appropriation of technology he was paid to work on as an SDG employee by filing for patents on them, naming himself as sole inventor. Notwithstanding Schwartz's resignation, SDG had little choice but to engage him as a paid consultant for SDG with respect to certain projects on which he was the designated Professional Engineer and replacing him would have been ruinous for SDG. What SDG did not realize at the time, however, was that Schwartz agreed to "help" SDG in this manner because he needed the $100,000 to finance the businesses he was establishing to compete with SDG.

Indeed, SDG subsequently learned that one of the expenses Schwartz paid with the $100,000 fee he charged SDG to avoid a complete breakdown of projects for which he was responsible on SDG's behalf were costs related to prosecuting "Schwartz's" patents on the concealment technology he developed while working for SDG. Although Schwartz, at or around the time of his resignation, began a campaign to solicit senior SDG engineers to leave SDG, the most experienced and capable SDG engineers refused his entreaties. Ultimately, however, Schwartz prevailed on defendants Hernandez, McGinley and Waldron to conspire with him to abuse their access to the SDG's business, technology and data and misappropriate proprietary information from SDG while establishing and even doing work for defendants Ahead Engineering and Far Field. Like Schwartz, defendants Hernandez, McGinley and Waldron had all been former employees of SDG's predecessor who remained with SDG when it was spun off in 2017. Hernandez began his relationship with the company in 2010 and McGinley was

employed starting in 2013; both were project managers at SDG. Ryan Waldron was employed by SDG as an engineer, having joined SDG's predecessor in 2015.

As detailed below, defendants were, and remain, brazen regarding their actions, except to the extent of hiding their wholesale removal of files from SDG's computers while they were working for SDG. This lack of shame on defendants' part extended to the manner in which they promote their new enterprises. For example, Ahead Engineering states on its LinkedIn profile that "Clients feel confident asking AE for advice on how new technology will work in the field. Having designed over 10,000 sites, our engineers have seen it all and our lessons learned drive our innovative spirit." Defendants, of course, know well that none of them individually, nor all of them combined, have experience with "10,000 sites," and that their claimed "10,000 sites" – and the associated data, designs and analytics about them – are SDG's, based on over 20 years of engineering and design work by SDS and its predecessor.

The Downloads and the Messaging

The electronic record of deceit, bad faith and untrammeled larceny left on SDG's computers by the individual defendants, all of whom are technically sophisticated yet who evinced no interest or concern regarding the detection of their actions following their departures, is stunning. That record is also exceedingly voluminous, and the few examples given here are meant to be exemplary only.

While employed by SDG, defendant Daniel Hernandez installed Facebook Messenger on his SDG computer, regarding which, of course, he had no expectation of privacy. Hernandez did not even bother to sign out of Facebook after resigning from SDG, much less delete the application or its data. As a result, after Hernandez's resignation SDG's network administrator encountered, without any effort, weeks' worth of date-stamped Facebook messages sent to and

from Hernandez by other the defendants, and to each other, concerning their conduct. SDG was able to corroborate much of what was described, including the defendants' removal of portable storage devices such as flash drives from users' computers, by routine use of the auditing function of SDG's Windows domain operating system.

The most remarkable and revealing cluster of Facebook messages revealing the unlawful conduct and disloyalty of the members of the defendants' conspiracy took place during the week prior to the mass resignation by Hernandez, McGinley and Waldron on January 16th. The first burst of Facebook Messenger activity on Hernandez's SDG computer during that week takes place on January 8, 2018, when Chad Schwartz announces to the group, "We got another 8 Extenet sites that I will walk this Thursday. That'll put us over $20,000 for the year so far (counting the sites [defendant] Ryan [Waldron] and I did just before the new year)." Defendant Waldron, whom Schwartz describes as having helped the group "get" one or more ExteNet sites, was, of course, still employed by SDG at the time. Later that day, defendant Hernandez reports to the group with enthusiasm about his prospect of snatching PSE&G, another client of his employer: "John just talked to me and next week I'll be meeting with pse&g to get pole work from them. We have to get this work for us!" Defendant Waldron expresses his pleasure. The same night, Schwartz coaches defendant Hernandez on the process of surreptitiously emptying his office before his planned resignation, telling Hernandez to take things out of the office slowly, the way Schwartz did. "By the time I actually quit, I didn't have the walk of shame, carrying out large file boxes," advises Schwartz.

The next day, January 9th, Schwartz crows to the group, "I just got another $150,000 worth of work promised to me. This feels too easy! [Defendant] Ryan [Waldron] needs to quit soon!!!" Schwartz explains, in response to a question from Hernandez, that this work came

from ExteNet and repeats to defendant Waldron the recommendation he made to Hernandez that he "start slowly removing your property," adding, with reference to his consulting fee from SDG, "As soon as I get the $ from SDG, you are free to go. ..." Tempering the exultation, later on that night Schwartz discusses the status of the formal formation of the new competitors to SDG with the SDG employees Hernandez, McGinley and Waldron, observing cynically – and inaccurately, "Also, [it]'d be wise to have non-competes and non-solicits for partners/employees for all members in both companies. Does anybody have an issue with that? That'd mean you can't go off on your own, steal clients, employees and compete with the other partners. These are things that SDG is wishing that they had about now." Inappropriately confident of what he believe is legal acumen on his part, Schwartz continues later in the discussion, "What if I take all [Ahead Engineering]'s clients and start my own company doing the exact same thing? Would you want me to do that to you? Well, guess what. I wouldn't want you to do it to me, either. And, SDG is pretty sorry that they didn't lock me down too."

The next day, Wednesday, January 10th, the group starts discussing its big plans for the coming weekend, ahead of the mass resignation that would take place on the following Tuesday, January 16th. One of Schwartz's new partners, Professional Engineer Taqi Khawaja, calls the proceedings to order at 10:53 a.m. – the middle of the work day at SDG – stating, "I think we have a lot to accomplish this weekend. Everyone should come with questions ready for accountant. We are meeting at 12pm right? That way we can set up our computers before the accountant gets there." The group discusses its plans. Later that afternoon, defendant McGinley shares with the group the news that, as hoped, ExteNet is moving all its business from SDG to Ahead Engineering, saying that Pat, an SDG employee, "just told Danny Hernandez and I that he doesn't think SDG is getting anything new from Extenet again, and the sites that they have POs

on but no drawings are most likely going away. He called [ExteNet's] Mary Jo and she said she wants to give the drawings to SDG, 'But you know the relationship [her superior at ExteNet] Sam and Chad have.'" After appreciation of this report, the group began discussing the process of locating and downloading, for their use, files and data located on the SDG server while they still had access to them, with Taqi Khawaja asking, "Any chance I could get that snow load calculation spread sheet from SDG? Doing a snow load set up right now . . ." Hernandez responds, "Check your email and let me know if that works." A short time later, after additional discussion – including a suggestion that Hernandez check SDG project files from 2010-12 for these engineering specifications – Hernandez tells Khawaja to check his email, which should contain three SDG project data spreadsheets Hernandez has simply stolen and sent to him. Indeed, says Khawaja, "one of them was it, thanks!"

ExteNet and PSE&G were not the only SDG client the defendants were soliciting to move to SDG's competitors. On January 9, 2018, defendant Hernandez announced to the Facebook chat group that another download mission had been accomplished: The raiding of SDG's database for material necessary to detach SDG from its client Tilson Technology Management. "Basic details, structural seed, tilson specs, tilson misc and other misc specs copied to flash drive." Although defendant Waldron expressed niggling reservations – "how about wireless specs?" – Hernandez dutifully promised to fetch them as soon as Waldron clarified what to look for. The espionage by defendant Hernandez bore fruit. On January 12, 2018, defendant Hernandez reports, "I got a call from Ben @ Tilson. He let me know the engines are going to be on full throttle this yr. He didn't tell me how many sites but it should be nice." His leader defendant Schwartz pats him on the back and follows up with a request for the contact information from SDG's system necessary to close the deal. Hernandez complies loyally.

Defendant Waldron's SDG computer demonstrates how the defendants applied the *coup de grâce* to the SDG / Tilson relationship, showing, in the "Recent Places" window automatically generated by Windows File Explorer, that Waldron accessed a key Tilson file on SDG's network before he left SDG. Indeed, throughout this period, the Facebook plotters still employed by SDG were assiduously downloading SDG site, engineering and client data to destroy SDG's business. For example, the Windows domain audit record of defendant Hernandez's portable storage use at his workstation confirms that he attached a portable storage device to it at 3:13 PM on January 9, 2018, corresponding his proud announcement of having. The audit trail of defendants' computers reveals many such instances. For example, Hernandez attached another flash drive or other portable storage device to his computer at 5:36 PM on January 15, 2018, after discussing, in the Facebook chat earlier that afternoon, the location of "drawings" on the SDG network.

In fact, SDG eventually learned that defendants' misappropriations began far earlier than the second week in January. For example, on December 29, 2017, in response to an inquiry by Taki Khawaja, defendant McGinley says, "let me know if you need me to access the server to send an example. I'll also look for NJ, NYC, NYS and PA non-ExteNet sites for reference." Defendant Waldron replies, "I should have some Extenet examples. I'll send a few of them over to Taqi soon." Ever helpful, Waldron asks, "Sure. Do you guys want the CAD too or just the PDF?" Defendant Waldron writes, a bit later, "Just sent three Extenet sites from Brooklyn," to which Robert Pietrocola, currently Director at Ahead Engineering, replies, "Awesome."

As early as December 27, 2017, the Facebook conspirators were actively discussing – seemingly interminably – the merits of a series of proposed logos and color schemes for their new companies, website copy and biographies, approaches to prospective clients (defendant

McGinley: "I'm reaching out to CAD outsourcing companies and would like to indicate our experience in the telecom world"), office equipment needs (McGinley: "does anyone have a large dry erase board? if not I'll go get one for the office. could be good for organizing tasks and projects") and departure dates. On January 2, 2018, defendant Schwartz announced to the group, "Ahead Engineering LLC is officially registered!" Schwartz is now President of Ahead Engineering and Far Field. And when, on January 16, 2018, Hernandez, McGinley and Waldron resigned from their positions at SDG, they officially became, respectively, Principal of defendant Far Field, Director of Engineering for defendant Ahead Engineering, and Director of Business Processes for defendant Far Field.

On February 21, 2018, counsel for SDG corresponded with each of the defendants and demanded that they cease their unlawful conduct, return all materials and proprietary information to SDG, preserve all relevant documentation and confirm their compliance with those demands within three days of that date. Defendants have not complied with these demands or in any way indicated their intention to do so. It is for this Court to do justice and apply equity and to protect what is left of SDG from this band of cynical, disloyal former employees and restrain their unethical and unlawful idea of how to compete in the free market: By stealing.

LEGAL ARGUMENT

I. SDG IS ENTITLED TO A TEMPORARY RESTRAINING ORDER AND A PRELIMINARY INJUNCTION

The standards for granting a restraining order and a preliminary injunction in New Jersey are well established. The Court must consider: (1) the likelihood of success on the merits; (2) whether irreparable harm will occur in the absence of preliminary relief; and (3) the relative hardship to the parties in granting or denying the relief. *Crowe v. DeGoia*, 90 N.J. 126, 133-34

(1982). Here, as demonstrated below and set out in vivid detail in the Verified Complaint, all these criteria favor the granting of the requested relief.

A. SDG will suffer irreparable harm if not granted a TRO

In general, loss of substantial business revenue – which the record shows has happened and, unless defendants are restrained, will continue to happen – constitutes irreparable harm for purposes of the issuance of preliminary injunctive relief. "Acts destroying a complainant's business, custom, and profits do an irreparable injury and authorize the issue of a preliminary injunction." *Ferraiuolo v. Manno,* 1 N.J. 105, 108 (1948), *citing*, *Vide Ideal Laundry Co. v. Gugliemona*, 107 N.J. Eq. 108, 110 (E. & A. 1930). In *Ferraiuolo,* the Court noted that even where the material facts were in dispute, an injunction would issue to preserve the *res* pending a final determination. The Court stated, "[O]ne of the exceptions to the stated rule is that the Court, having jurisdiction, will always intervene to protect the *res* from destruction, loss or impairment, so as to prevent the decree of the Court, upon the merits, from becoming futile or inefficacious in operation." *See also Silverstein v. Abco Vending Service*, 37 N.J. Super. 439, 446 (App. Div. 1955) ("There is nothing new about the appropriateness of the remedy of injunction to restrain acts destroying a complainant's business, custom a"@); *Russell v. Russell,* 127 N.J.Eq. 555, 559 (Ch. Div. 1940) ("There is absolutely no question about the power of this Court to protect a man in the exercise of his business, or calling, from which he derives his livelihood.")

In particular, New Jersey courts have never left any doubt as to whether disclosure – actual or threatened – of trade secrets, much less by former employees and much less by former employees whose disloyalty while working for the plaintiff has been shown, constitutes irreparable harm. A recent decision comprehensively summarized the relevant New Jersey law:

> It is a generally accepted principle that improper use or disclosure of an employer's trade secrets may constitute irreparable harm. *See Nat. Starch &*

> *Chem. v. Parker Chem. Corp.*, 219 N.J.Super. 158, 162 (App.Div.1987); *Sun Dial Corp. v. Rideout*, 16 N.J. 252, 259 (1954). Likewise, the diversion of a company's customers may also constitute irreparable harm. *J.I. Kislak, Inc. v. Artof.*, 13 N.J. Misc. 129, 132 (Ct. Ch.1935). This is so because the extent of the injury to the business as a result of this type of conduct cannot be readily ascertained, and as such, does not lend itself to a straightforward calculation of money damages. *National Starch*, 219 N.J.Super. at 163 (" '[D]amages will not be an adequate remedy where a competitor has obtained the secrets; the cat is out of the bag and there is no way of knowing to what extent their use has caused damage or loss" '); *J.I. Kislak, Inc.*, 13 N.J. Misc. at *id.* A finding of irreparable harm in these types of cases is appropriate even absent an express agreement between the parties safeguarding such information. *See Sun Dial Corp.*, 16 N.J. at 259 (holding that equitable intervention is appropriate where employees learn of an employer's trade secret in confidence, and use or disclose it in violation of such confidence after termination of their employment, despite the lack of an express agreement restraining their disclosure of trade secrets).
>
> Moreover, in the trade secrets context, an employer need not establish that its former employee has actually used or disclosed trade secrets. *National Starch, supra*, at 162. Instead, the employer may demonstrate that the ex-employee knows the trade secrets, and that under the circumstances, there is a sufficient likelihood of "inevitable disclosure" of its trade secrets to a competitor, which will likely result in irreparable harm. *Id.* ("The circumstances here justify **more than a "mere suspicion,"** and constitute a rational basis for the trial court to conclude that there was a sufficient threat of impending injury to warrant preliminary relief pending trial." *Id.*) In *National Starch*, for example, the Appellate Division affirmed the trial court's issuance of injunctive relief where sufficient evidence demonstrated that defendant, a former employee, learned the trade secrets of its employer, a company engaged in the envelope adhesion business, and subsequently went to work for an industry competitor. 219 N.J.Super. 158. . . .

Fluoramics, Inc. v. Trueba, No. BER-C-408-05, 2005 WL 3455185, at *8 (N.J. Super. Ct. Ch. Div. Dec. 16, 2005). Additionally, the New Jersey Trade Secrets Act explicitly authorizes injunctive relief to prevent and mitigate threatened or actual misappropriation of a trade secret.

There is little factual dispute regarding the facts here, because, as set forth in the Verified Complaint, the defendants freely acknowledged the facts that, while employees of SDG, they covertly established two firms to compete with their employer; that as employees of SDG they solicited clients and employees of SDG to leave SDG and by all indications continue to do so;

and that while employees of SDG they systematically ransacked SDG's computer network for proprietary client, specification, job-site and other valuable information to compete with SDG.

B. SDG is likely to succeed on the merits of its claims

"Where a plaintiff has established a *prima facie* case of wrongdoing by a defendant, New Jersey courts have, in a limited variety of contexts, afforded plaintiffs a presumption of liability, thereby shifting the burden of going forward to the defendant to rebut the presumption." *De Milio v. Schrager*, 285 N.J. Super. 183, 198 (Law Div. 1995). Here that test is also readily met on this record. We address the elements of the claims addressed by this motion *seriatim*.

SDG's first claim arises under the New Jersey Trade Secrets Act, N.J.S.A. § 56:15-1, *et seq.* (hereinafter, the "Act"), which prohibits the actual or threatened misappropriation of a "trade secret." N.J.S.A. § 56:15–3. A "trade secret," in turn, is defined as "information" that (1) "[d]erives 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," and (2) that the holder reasonably endeavors to maintain as confidential. N.J.S.A. § 56:15-2. The Act defines misappropriation of a trade secret as:

> (1) Acquisition of a trade secret of another by a person who knows or has reason to know that a person acquired the trade secret by improper means; or
>
> (2) Disclosure or use of a trade secret of another without express or implied consent of the trade secret owner by a person who:
>
> (a) Used improper means to acquire knowledge of the trade secret; or
>
> (b) At the time of disclosure or use, knew or had reason to know that the knowledge of the trade secret was derived or acquired through improper means; or

(c) Before a material change of position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired through improper means.

Under the facts here, defendants repeatedly and maliciously violated the N.J. Trade Secrets Act.

So too regarding SDG's claims based on breach of the duty of loyalty and related torts of competition. As our Supreme Court recently stated in *Kaye v. Rosefielde*, 223 N.J. 218 (2015):

> As this Court has observed, "[l]oyalty from an employee to an employer consists of certain very basic and common sense obligations. An employee must not while employed act contrary to the employer's interest." . . .
>
> The Court's most detailed analysis of the duty of loyalty was set forth in its opinion in *Cameco*[*, Inc. v. Gedicke, 157 N.J. 504, 724 A.2d 783 (1999)*]. . . . .
>
> To guide trial courts, the Court identified four factors relevant to the determination of whether an employee-agent breached his or her duty of loyalty: 1) the "existence of contractual provisions" relevant to the employee's actions; 2) the employer's knowledge of, or agreement to, the employee's actions; 3) the "status of the employee and his or her relationship to the employer," e.g., corporate officer or director versus production line worker; and 4) the "nature of the employee's [conduct] and its effect on the employer." *Id.* at 521–22; *see also Lamorte, supra*, 167 *N.J.* at 303 (noting factors). Thus, a trial court considers the parties' expectations of the services that the employee will perform in return for his or her compensation, as well as the "egregiousness" of the misconduct that leads to the claim. *Cameco, supra*, 157 *N.J.* at 521–22.

223 N.J. 218, 229-230. Here, while there were no written contracts governing the defendants' conduct vis-à-vis competition with SDG, the other three Cameco factors so profoundly favor plaintiff that the lack of a contract is immaterial. SDG did not know about its employees' establishment of a competing company, much less their supplying of that company with its proprietary methods and data and its solicitation of important clients. "To avoid the possibility of charges of disloyalty, employees generally should inform employers of their plans before establishing an independent business that might conflict with that of the employer. To an employee, the possibility of conflict with the employer's interest may seem remote; to the employer, the possibility may seem more immediate. The greater the possibility that another

occupation will conflict with the employee's duties to the employer, the greater the need for the employee to alert the employer to that possibility." *Cameco, id*., 57 N.J. at 517.

Regarding the other *Cameco* factors, all the individual defendants here are professionals; all but one was the engineering equivalent of a vice president, i.e., a project manager or higher. And the nature of the disloyalty here and its effect on SDG have been profound, as set out above: The loss of several key clients, key employees, inestimable proprietary data and millions of dollars in revenue. These are more than enough to establish a likelihood of success under *Cameco*, as the court found in *Platinum Mgmt., Inc. v. Dahms*, 285 N.J. Super. 274, 305 (Law. Div. 1995). There the defendants, wrote the court, "while still employed by [plaintiff] and enjoying its trust and the benefits of their employment, in effect went into secret competition with their employer. . . .[T]heir conduct furthered [their new company's]'s competitive advantage while they were still employed by [plaintiff], a clear breach of their duty of loyalty to PMI." Secret competitionwith an employer, with exactly the same results, is exactly what happened here. No written agreement is required to know it is wrong, or to prevent and punish it.

Moreover, there is a special duty of employee loyalty relating to the maintenance of corporate confidentiality. "[E]mployees have a common law duty to safeguard confidential information they have learned through their employment relationship and that they are generally precluded from sharing that information with unauthorized third parties." *Quinlan v. Curtiss-Wright Cor*p., 204 N.J. 239, 260 (2010). On this point, too, contrary to the arrogant assurances broadcast by defendant Schwartz, no written policy, employment contract or employee handbook is necessary to protect an employer from such misappropriation.

New Jersey law does not only prohibit what occurred here under trade secrets law and the common-sense common law of employee loyalty. As the court explained in *Platinum Mgmt,*

when such a conspiracy, involving as it does "a deliberate plan" on the part of the new employer and the former employees "to cause damage to [the original employer] through diversion of its customers at a time critical to PMI in selling to these customers," those involved are also liable for tortious interference with prospective economic advantage. 285 N.J. Super. at 306.

C. Weighing the relative hardship of the parties favors SDG

SDG has been hollowed out from the inside by the loss of critical staff, proprietary information and important client relationships, all caused not only by the departure of the four faithless employees named as defendants here but their cynical scheme to steal every one of those valuable assets while employed for purposes of establishing competing businesses. "Courts have recognized the damage a former disloyal employee is able to inflict on his employer, even in the absence of a covenant, where he has launched or assisted a competing business while he is employed." *Platinum Mgmt., id.*. at 303.

II. DEFENDANTS HAD NO REASONABLE EXPECTATION OF PRIVACY CONCERNING THE INFORMATION LEFT ON THE SDG COMPUTERS USED BY THEM.

Much of the information in the Verified Complaint comes from the SDG-owned computers of the individual defendants, as is typically the case in conflicts of this nature in the 21st century. The admissibility of such evidence, and the propriety from a privacy point of view of SDG's use of this information – including the open chat discussion left by defendant Daniel Hernandez on his SDG computer after his resignation – is beyond cavil. "Relevant information in the private section of a social media account is discoverable. It is not privileged nor protected from production by a common law right of privacy." *Howell v. Buckeye Ranch, Inc*., No. 2:11-CV-1014, 2012 WL 5265170, at *1 (S.D. Ohio Oct. 1, 2012) (citing *Glazer v. Fireman's Fund*

Insurance Company, 2012 WL 1197167, *3–*4 (S.D.N.Y. April 5, 2012) and *Tompkins v. Detroit Metropolitan Airport*, 278 F.R.D. 387, 388 (E.D.Mich.2012)

For this reason, the Appellate Division has ruled, "We need not create a new test for social media postings. Defendant argues a tweet can be easily forged, but so can a letter or any other kind of writing. The simple fact that a tweet is created on the Internet does not set it apart from other writings. Accordingly, we apply our traditional rules of authentication under N.J.R.E. 901." *State v. Hanna*h, 448 N.J. Super. 78, 89 (App. Div. 2016). Therefore comments in defendants' Facebook chat would be discoverable and admissible in this case just as any other "private," unprivileged communications would be. *See also, Beye v. Horizon Blue Cross Blue Shield of New Jersey*, No. CIV.A. 06-5337-FSH, 2007 WL 7393489, at *2 (D.N.J. Dec. 14, 2007) (requiring production of entries on social media that were shared with others).

In this case, moreover, SDG did not need to wait until these chats were produced in discovery because it is entitled to directly inspect information stored, unsecured, on its own computers that are used by its employees. An employer has a legitimate interest in monitoring unsecured communications on computers used by employees. *Liebeskind v. Rutgers Univ*., No. A-0544-12T1, 2014 WL 7662032, at *7 (N.J. Super. Ct. App. Div. Jan. 22, 2015). The leading case in New Jersey on this topic is *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300 (2010), in which the Supreme Court held that employers can monitor and regulate the use of workplace computers because they have a legitimate interest to protect their assets, reputation, and business productivity – exactly the interests being vitiated by this action. The employee in *Stengart* was found to a reasonable expectation of privacy regarding conspicuous as attorney-client communications in a password-protected account whose login credentials were not left on the company computer, but the Court was at pains to note that its ruling "does not mean that

employers cannot monitor or regulate the use of workplace computers." *Id*. at 324. Thus where, as here, an employer had a legitimate interest in monitoring and regulating plaintiff's workplace computer – which can never be the case regarding attorney-client communications – and, critically, SDG did not try to access the content of personal, password-protected accounts, Hernandez did not have a reasonable expectation of privacy concerning these chats.

Furthermore, there is never a reasonable expectation of privacy where, as here, the one claiming it allows access to supposedly private information to another party. *Hall v. Heavey*, 195 N.J. Super. 590, 597 (App. Div. 1984). Here the fact that the Facebook chat was, as attested to by the certification of Jason Gerstenfeld, SDG's IT director, found on an SDG computer – unsecured and accessible for viewing by anyone logging onto the computer – vitiates any potential privacy objection. These communications were basically handed to SDG by being left on Hernandez's computer upon his departure. In such a case, no serious claim can be made that the employee reasonably expected them to remain private.

Almost this precise scenario – where a party claimed to have an expectation of privacy with respect to communications left unsecured because the user failed to log out of a computer accessible to others – occurred in *Marcus v. Rogers*, No. A-2937-09T3, 2012 WL 2428046, at *5 (N.J. Super. Ct. App. Div. June 28, 2012). The Appellate Division rejected the privacy claim, stating, "Because the index to the inbox of Marcus's Yahoo e-mail was displayed on the screen when the last user left the computer, Wayne did not access the facility without authorization. The accessing of the facility on which Marcus's e-mail was stored and the display of its index had been accomplished by the last user of the computer, which we must presume was Marcus because there is no evidence of hacking or misuse of her password." The same applies here, where Hernandez was the last user of the SDG computer on which his Facebook chat was left

open. *See also*, *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 674 (D.N.J. 2013) (no actionable violation of an employee's privacy when an employer simply accessed information on Facebook that had not been secured); *White v. White*, 344 N.J. Super. 211, 221 (Ch. Div. 2001) ("[D]efendant did not use plaintiff's password or code without authorization. Rather, she accessed the information in question by roaming in and out of different directories on the hard drive. [W]here a party consents to another's access to its computer network, it cannot claim that such access was unauthorized" (citation and internal quotes omitted).

III. SDG IS ENTITLED TO EXPEDITED DISCOVERY.

The Court has discretion to order expedited discovery, and given the quality of the evidence and the indicia of bad faith by defendants doing is be appropriate here to ascertain what files and date were removed from SDG and converted to the use of defendants, what clients of SDG were improperly contacted by defendants – especially those who did so disloyally, while employees of SDG – and, to the extent possible, what they were told; to arrange for prompt forensic inspection of all media, data and computers relevant to the claims; and to salvage SDG's business from the pirates who misappropriated it for themselves and beat their chests about it.

CONCLUSION

For all of the foregoing reasons, and for the reasons set forth in the Verified Complaint, this Court should issue a temporary restraining order and a preliminary injunction ordering (a) expedited discovery; 2) non-solicitation by defendants of all SDG clients and employees; 3) returning all files, data and things that are the property of SDG and which have been converted and are unlawfully possessed by defendants; and (4) preserving all relevant data and media.

MANDELBAUM SALSBURG P.C.

By: 
Ronald D. Coleman

3 Becker Farm Road
Roseland, NJ 07068
973-736-4600
rcoleman@lawfirm.ms
Attorneys for Plaintiff
Scherer Design Group, LLC