SUPERIOR COURT OF NEW JERSEY
APPELLATE DIVISION
DOCKET NO. A-2933-15T3

eMAZZANTI TECHNOLOGIES, INC.,

Plaintiff-Respondent,

v.

DOUGLAS SINGER AND NICHE SERVICES, LLC,[1]

Defendants-Appellants.

Argued November 28, 2017 – Decided February 23, 2018

Before Judges Sumners and Moynihan.

On appeal from Superior Court of New Jersey, Law Division, Hudson County, Docket No. L-1974-13.

Alissa Pyrich argued the cause for appellant (Jardim, Meisner & Susser, PC, attorneys; Anthony Bedwell and Alissa Pyrich, of counsel and on the brief; Tracy U. Azinge, on the briefs).

Kerry B. Flowers argued the cause for respondent (Flowers & O'Brien, LLC, attorneys; Kerry B. Flowers and Michele A. Daitz, of counsel and on the brief).

---

[1] Although Niche Services, LLC, is listed as an appellant in the notice of appeal, the order on appeal applies only to Douglas Singer.

PER CURIAM

Following a ten-day bench trial, Judge Kimberly Espinales-Maloney issued an order of judgment in favor of plaintiff eMazzanti Technologies, Inc. (eMazzanti or company) against defendant Douglas Singer, its former employee, for $27,200 in compensatory damages under N.J.S.A. 2A:38A-3. The statute is part of the New Jersey Computer Related Offenses Act (CROA), N.J.S.A. 2A:38A-1 to -6, which permits a business owner to recover compensatory and punitive damages, and attorney's fees and costs, for the purposeful or knowing alteration, taking, destruction, damage, and unauthorized tampering with its computer or computer system.[2] The

[2] N.J.S.A. 2A:38A-3 provides:

> A person or enterprise damaged in business or property as a result of any of the following actions may sue the actor therefor in the Superior Court and may recover compensatory and punitive damages and the cost of the suit including a reasonable attorney's fee, costs of investigation and litigation:
>
> a. The purposeful or knowing, and unauthorized altering, damaging, taking or destruction of any data, data base, computer program, computer software or computer equipment existing internally or externally to a computer, computer system or computer network;
>
> b. The purposeful or knowing, and unauthorized altering, damaging, taking or destroying of a computer, computer system or computer network;

judge determined that Singer had accessed eMazzanti's computer system without authorization, and took and destroyed electronic data information therefrom. Three months later, the judge granted eMazzanti's motions for attorneys' fees, cost of suits, and punitive damages under the statute.

Before us, Singer contends eMazzanti should not have been awarded compensatory damages because the judge's credibility findings in favor of eMazzanti were against the weight of the evidence, and the judge abused her discretion in allowing the admission of certain evidence. He furthers argues eMazzanti failed to prove entitlement to punitive damages by clear and convincing evidence. We disagree and affirm.

> c. The purposeful or knowing, and unauthorized accessing or attempt to access any computer, computer system or computer network;
>
> d. The purposeful or knowing, and unauthorized altering, accessing, tampering with, obtaining, intercepting, damaging or destroying of a financial instrument; or
>
> e. The purposeful or knowing accessing and reckless altering, damaging, destroying or obtaining of any data, data base, computer, computer program, computer software, computer equipment, computer system or computer network.

eMazzanti is an information technology services company involved in designing, upgrading, maintaining, and monitoring of clients' computer network infrastructure; consulting clients on securing, implementing and improving their computer networks; storing and providing back-up services for clients' digital assets; and setting up wireless infrastructures to enable remote and mobile access. The company, owned by husband and wife, Carl and Jennifer Mazzanti (Mazzanti, hereinafter refers solely to Carl), employed Singer as Senior Network Engineer and Project Team Lead for ten years. As a condition of employment, Singer, like other employees, signed a non-disclosure agreement to ensure the privacy of eMazzanti's clients' confidential and proprietary electronic information that was maintained to service clients' needs. The company also implemented security measures to prevent employees from unauthorized access to client data, including data encryption, heightened password and authentication requirements, alerts for each login, and a ticketing system that tracked access and use of client data. Only Singer and Mazzanti had access to the "Domain Controller," the central security point for eMazzanti's computer system[3] to control access levels to the

[3] When discussing eMazzanti's "computer system" or "computer network" herein, these terms are interchangeable and generally refer to eMazzanti's digital computer infrastructure, which includes its computer programs, software, files, and servers.

system's files, folder, accounting data, customer lists, and everything from e-mail. However, Singer did not have access to data stored on plaintiff's server or other employees' email communications stored on the email exchange server.

On February 21, 2002, following an upsetting meeting with the Mazzantis, Singer left work and did not return until two days later. According to Mazzanti's testimony, during Singer's first day of absence, Mazzanti was repeatedly kicked out of the company's computer system, indicating another user was logged into the same account at the same time. On February 23, at 12:23 a.m., the morning prior to Singer's return, Mazzanti logged into the Domain Controller remotely from his home, and discovered that Singer had logged into the Domain Controller administrative account at approximately 10:00 a.m. on February 22 and remained logged in for one day, fourteen hours and seven minutes. In addition, the email exchange server showed that Singer had accessed it, and remained logged in for one day, fourteen hours, and forty-five minutes.

Mazzanti also claimed the back-up hard drive for the company's server was missing from the server room, to which only he and Singer had access. The camera system's login list showed two administrative account logins occurred on February 23, at 10:33 a.m. and 5:04 p.m., but did not specify any username. When Mazzanti reviewed the camera footage from the server room, he

discovered the recordings for that week were deleted. By logging into the camera system, a person could delete its recordings. Mazzanti claimed that he did not go into the server room, and surmised that Singer did so.

When Singer returned to work, Mazzanti terminated his employment for violating company policy by accessing computer files and employees' emails without authorization. Mazzanti maintained that Singer had only been given such access to the Domain Controller seven years prior, because Mazzanti was on his honeymoon in Egypt without computer access, so that Singer would be able to fix any problems during Mazzanti's absence. Thereafter, Mazzanti contended he told Singer that he was not allowed to access the Domain Controller without authorization, and if he did, he would be terminated.

In evidence, Mazzanti presented screenshots that he took of Singer's computer screen when Singer was out of work depicting Singer's remote activity on the company's system during the two days prior to his termination, which led Mazzanti to conclude Singer accessed the system without authority.

To further support the claim that Singer was aware he needed authorization to access the computer system, there was a "legal warning" that appeared each time an employee logged onto the

computer system, requiring the employee to accept its terms before logging in. The warning stated:

> This computer system is operated by eMazzanti and may be accessed only by authorized users. Authorized users are granted specific, limited privileges in the use of the system. The data and programs in this system may not be accessed, copied, modified or disclosed without prior approval of eMazzanti, Inc. Access and use, or causing access and use, of this computer system by anyone other than as permitted by eMazzanti are strictly prohibited by eMazzanti and by law and may subject an unauthorized user, including unauthorized employees, to criminal and civil penalties. The use of this system is routinely monitored and recorded.

Mazzanti testified his company had to shut down for a week following Singer's breach to ensure the security of its clients' and the company's confidential electronic information. Two weeks after Singer's termination, Mazzanti received Singer's company-owned laptop in the mail. The laptop's hard drives were cleaned of Singer's profile and all of its data, thereby preventing an assessment of Singer's activity on the laptop. Over a month later, Singer established his own information technology company, Niche, to provide the same services as offered by eMazzanti. In fact, one of eMazzanti's former clients became Niche's client.

Based upon his investigation, Mazzanti concluded Singer exceeded his computer privileges by reading employees' emails and accessing the system without authorization.

Singer, referencing the access given to him during Mazzanti's honeymoon, denied Mazzanti's assertion that he needed Mazzanti's permission to access the domain account. However, Halim Dumi, an employee of eMazzanti, who worked with Singer before Singer was terminated, and took over Singer's job, confirmed Mazzanti's testimony of the company-wide access restriction policies, including the access restrictions articulated in the Employee Handbook and the pop-up legal warning. Singer also denied that he was accessing eMazzanti's computer system remotely when he was out of work two days prior to his termination; claiming he merely did not log out of the system after working on tasks for the company and clients and going home. To the contrary, Mazzanti maintained that the screenshots showed that Singer was active on the system remotely.

In her detailed written decision, Judge Espinales-Maloney assessed the witnesses' testimony and found Mazzanti's and Dumi's testimony more credible than Singer's denials. She reasoned Mazzanti's demeanor "was calm, direct, assertive, and without hesitation" and his "testimony regarding Singer's actions on February 23, 2012 [was] consistent with the trial exhibits." She therefore determined Singer violated N.J.S.A. 2A:38A-3 by accessing eMazzanti's Domain Controller, client servers, and email exchange server, without authorization. We defer to the judge's

ability to hear "the witnesses, sift[] [through] the competing evidence, and [make] reasoned conclusions." Griepenburg v. Twp. of Ocean, 220 N.J. 239, 254 (2015). We therefore discern no reason to upset her factual findings because we are unpersuaded that they were "so manifestly unsupported by or inconsistent with the competent, relevant and reasonably credible evidence as to offend the interests of justice." Ibid. (citations omitted). Accordingly, we reject Singer's effort to have us assess the evidence and make independent findings of Mazzanti's credibility and the weight given to the screenshots from eMazzanti's camera system, the Domain Controller and the email exchange server. See Cannuscio v. Claridge Hotel & Casino, 319 N.J. Super. 342, 347 (App. Div. 1999).

Next, we address Singer's argument that the judge abused her discretion in allowing Mazzanti to testify regarding evidence that was not produced in discovery-Mazzanti's testimony regarding the screenshots, and the alerts he was getting for access privileges from Singer's account. We see no abuse of discretion.

Singer's concerns were initially addressed in pre-trial in limine motions when Judge Espinales-Maloney found defendants "never filed a motion to dismiss or compel the documents any time during discovery, as required by Rule 4:18-1 and 4:24-2" despite receiving the documents four months prior to trial, and they

instead "sat on their rights for four months, essentially lying in wait." The judge further determined there was good cause and no attempt to mislead by not forwarding the documents prior to the end of discovery.[4] We take no issue with the judge's decision to admit the late-produced documents "[i]n the interest of justice to hear the case on the merits" and "decide this case based on all of the credible evidence." The judge gave a rational explanation that was consistent with our rules and did not constitute an injustice to Singer. Hisenaj v. Kuehner, 194 N.J. 6, 20 (2008); Jacoby v. Jacoby, 427 N.J. Super. 109, 116 (App. Div. 2012).

Moreover, during the trial, following the parties' conference in chambers with the judge, defense counsel withdrew his objections to the documents, stipulated to their admission, and in fact, stated his intention to use the documents in Singer's case in chief. Thus, even if the documents' admission was improper, under the doctrine of invited error, Singer cannot now assert that Mazzanti's testimony regarding the documents was improper. Brett v. Great Am. Rec., Inc., 144 N.J. 479, 503 (1996) ("The doctrine of invited error operates to bar a disappointed litigant from arguing on appeal that an adverse decision below was the product

[4] The tardy production was a result of eMazzanti's counsel being consumed with her husband's medical issues and sudden death.

of error, when that party urged the lower court to adopt the proposition now alleged to be error.").

Any arguments not addressed concerning the weighing of evidence and admission of evidence lack sufficient merit to warrant discussion in a written opinion. R. 2:11-3(e)(1)(E). In summary, we conclude the record contains sufficient credible evidence supporting Judge Espinales-Maloney's findings that Singer violated CROA and eMazzanti is entitled to the compensatory damages awarded.

Finally, there is no merit to Singer's arguments that punitive damages were not warranted because there was insufficient evidence that he "acted egregiously or with an evil mind" and no evidence that he made unauthorized access to eMazzanti's computer system and he deleted information on his company-issued laptop. Since we noted above that the record contains sufficient credible evidence supporting the finding that Singer violated CROA, we do not address Singer's repeated attack on the sufficiency of the evidence.

Singer's contention that punitive damages were awarded based on the finding that his actions were egregious or with evil intentions is misplaced. In awarding punitive damages, the judge

applied the Punitive Damages Act,[5] specifically N.J.S.A. 2A:15-5.12(a), which provides:

> Punitive damages may be awarded to the plaintiff only if the plaintiff proves, by clear and convincing evidence, that the harm suffered was the result of the defendant's acts or omissions, and such acts or omissions were actuated by actual malice or accompanied by a wanton and willful disregard of persons who foreseeably might be harmed by those acts or omissions. This burden of proof may not be satisfied by proof of any degree of negligence including gross negligence.
>
> [(Emphasis added).]

Thus, the judge did not, and need not have found, Singer acted with "actual malice" as he contends, to determine he was liable for punitive damages. We conclude the punitive damages award does not result "in a manifest denial of justice," Maul v. Kirkman, 270 N.J. Super. 596, 620 (App. Div. 1994), because the record supports the judge's finding that there was clear and convincing evidence that Singer acted with "wanton and willful disregard . . . which had a high probability of damaging eMazzanti's business" and demonstrated his "reckless indifference to the harm that eMazzanti would suffer."

Affirmed.

[5] N.J.S.A. 2A:15-5.9 to -5.17.