IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

SECURE DATA TECHNOLOGIES, INC.	)	
	)	
Plaintiff	)	
	)	
v.	)	CASE NO. 4:20-1228
	)	
JAMIE STEPHANIE GUILFORD	)	
	)	
&	)	
	)	
GUILFORD TECHNOLOGIES, LLC	)	
	)	
	)	JURY DEMAND
	)	
Defendants	)	

COMPLAINT

The Parties

1. Plaintiff Secure Data Technologies, Inc. (referred to herein as "Secure Data" and "Plaintiff") is an Illinois Corporation and citizen with its primary place of business located at 1392 Frontage Road, O'Fallon, St. Clair County, Illinois.

2. Defendant Jamie Stephanie Guilford (referred to herein as "Guilford") is a resident and citizen of Missouri, 856 Autumn Grove Dr., O'Fallon, Missouri 63365.

3. Defendant Guilford Technologies, LLC ("hereto refereed as Guilford Technologies") is a Missouri Limited Liability Corporation, a citizen of the State of Missouri, formed in May, 2020, with its primary place of business located at 856 Autumn Grove Dr., O'Fallon, Missouri 63365. Defendant Jamie Guilford is its CEO and registered agent.

Nature of the Action

4. This civil action is for Breach of Contract (Count I), Tortious Interference with Plaintiff's Contracts and/or Business Expectancies (Count II), Unjust Enrichment (Count III), Misappropriation of Trade Secrets in Violation of the Illinois Uniform Trade Secrets Act, ("ITSA") (765 ILCS 1065/1 *et seq*)). (Count IV), Violations of Stored Wire and Electronic Communications Act ("SECA"), 18 U.S.C. § 2701, *et seq*. (Count V), Violations of Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, *et seq*. (Count VI), Violation of the Missouri Statute Against Tampering with Computer Data and Equipment, R.S. Mo. § 537.525, and the Missouri Statute Against Tampering with Computer Equipment, R.S. Mo. § 569.097 (Count VII).

Jurisdiction and Venue

5. This Court has original diversity jurisdiction of the instant matter pursuant to 28 U.S.C.§1332 for it is a civil action where the matter in controversy exceeds the sum or value of $75,000, exclusive of interest and costs, and is between citizens of different States. Plaintiff Secure Data is a citizen of Illinois. Defendants Guilford and Guilford Technologies are Missouri citizens. Additionally, This Court also has federal question jurisdiction over Counts VI and VII of this Complaint, which are claims under the Stored Wire and Electronic Communications Act ("SECA"), 18 U.S.C. § 2701 *et seq*. and the Computer Fraud & Abuse Act ("CFAA), 18 U.S.C.§ 1030 ei *seq*, respectively. This Court has supplemental jurisdiction over the remaining Counts.

6. Venue is appropriate in this Court inasmuch as the Plaintiff and Defendant Guilford resides or otherwise can be found within the District, the subject matter leading to the formation of his consulting business, a Missouri Limited Liability Company, was engaged in by Defendant Guilford within this District, the tampering with a computer occurred within this

district, and the causes of action against Defendant Guilford arise from multiple acts committed by Guilford in Missouri. This Court has personal jurisdiction over the Defendant who is a citizen of Missouri, residing in the Judicial District of the Eastern District of Missouri.

Facts Common to all Counts

7. Plaintiff Secure Data is an infrastructure technology company, which provides clients with hardware, software, managed services and professional services in four areas: Collaboration, Data Center, Network and Security.

8. Defendant Jamie Stephanie Guilford (referred to herein as "Guilford") was a salaried Senior Consulting System Engineer. Part of Guilford's job was to interface with secure data's client base, to work with wireless, security and Data center design, set up and integration.

9. Defendant Guilford Technologies is a direct competitor of Secure Data, formed and maintained by Guilford to provide consultative, infrastructure technology services.

10. Defendant Guilford work for Secure Data from the period of approximately July 9, 2018 to February 23, 2020 (beginning under her previous name Stephen Guilford), and now is employed by Guilford Technologies.

Guilford Illegally Hacked into Company Email

11. During the period of Guilford's employment with secure Data for which she was receiving salary, there were concerns raised within the company that Guilford improperly and without authorization hacked into the email accounts of Secure Data management.

12. Secure Data confirmed that prior to her termination, Guilford improperly and illegally hacked into Secure Data's communications system to review sensitive email exchanged among Secure Data's management team.

13. On the evening of February 23, 2020, Jeff Young of Secure Data was alerted to a possible security breach of Secure Data's email system. Upon reviewing audit logs, Young noticed that Guilford had provided herself unapproved access to the mailboxes of CEO Dana Steffey, CFO Derek Herbison and employee Simonne Meszaros

14. After additional review, Young confirmed that Guilford also accessed Young's own email mailbox without approval on February 21, 2020 and multiple other times the week of February 17, 2020.

15. On the evening of February 23, 2020, Young of Secure Data was alerted to a possible security breach of Secure Data's email system. Upon reviewing audit logs, Young noticed that Guilford had provided herself unapproved access to the mailboxes of CEO Dana Steffey, CFO Derek Herbison and employee Simonne Meszaros

16. After additional review, Young confirmed that Guilford also accessed Young's own email mailbox without approval on February 21, 2020 and multiple other times the week of February 17, 2020.

17. Attached hereto as Exhibit 2 and incorporated herein is an admission by Guilford that she illegally hacked into Secure Data's confidential emails.

18. Guilford was terminated from Secure Data as a result of her improper conduct.

The Non-Compete Agreement

19. Attached hereto as Exhibit 1 is an Employee Non-Compete Agreement entered into by Guilford with Secure Data on June 22, 2018.

20. Section 2 of said Non-Compete Agreement has the following terms in place concerning "Confidential Information":

2. Confidential Information.

(a) From and after the date of this Agreement (without limitation as to time), Employee shall treat as the Company's confidential information ("Confidential Information") all data, customer lists, information, ideas, knowledge and papers pertaining to the affairs of the Company which are not made public under the direction of the Company's management. Without limiting the generality of the foregoing, such Confidential Information shall include: the identity of customers; the identity of the Company's suppliers and prospective suppliers; the identity of the Company's creditors and financial backers or potential creditors and other potential financial backers; technical improvements, designs, inventions, methods, processes, techniques and skills, devised, developed or used by or for the Company; the Company's estimating and costing procedures and the cost and gross prices charged by the Company for its services; the prices or other consideration charged to or required of the Company by any of its suppliers or potential suppliers; and the Company's sales and promotional policies. Employee shall not reveal Confidential Information to others except in the proper exercise of Employee's duties and authority for the Company, nor use Employee's knowledge thereof in any way that would be detrimental to the interests of the Company. Employee shall also treat all information pertaining to the affairs of the Company's customers and suppliers with the same degree of confidentiality as he is obligated to treat the Confidential Information. Employee shall upon or prior to Employee's termination of employment with the Company turns over to the Company all copies of all documents, papers, memoranda, data, or other matter, whether published or unpublished and in whatever media they exist, which Employee may have or control relating to the Company or its customers, and that the same is and shall be the exclusive property of the Company and the Company shall be entitled to all copyright rights therein.

(b) All inventions, designs, discoveries, developments, improvements or other Confidential Information, whether or not patentable or subject to copyright, developed by Employee while an employee of the Company shall belong exclusively to the Company. Without limiting the foregoing, all copyrightable material produced by the Employee while an employee of the Company shall be deemed to be "works for hire" produced for the Company. Employee shall execute such other documents and perform (or cause to be performed) such other acts as the Employer may reasonably request in order to effectuate the provisions and intent of this paragraph and assist the Company in enforcing its rights in said inventions, designs, discoveries, developments, improvements or other Confidential Information.

(c) Employee covenants that Employee has not and will not use or disclose the confidential information of any of Employee's prior employers. Employee covenants that, by Employee's employment by the Company will not violate any agreement that Employee has with any of Employee's prior employers.

21. On March 2, 2020, Secure Data sent a letter via Certified Mail to Guilford, with a copy of the Non-Compete Agreement attached. The letter stated in part:

> Per paragraph 4, you are required to provide a copy of the Agreement to any prospective employer so that any such employer would not inadvertently cause the violation of the Agreement. I have provided a copy of the Agreement, so that you will be able to provide it to any current or prospective employer.
>
> As you can see, Paragraph 1 of the Agreement provides that for a period of one year following your departure from Secure Data, you will (a) not solicit or accept business from any entity that is a past, current or prospective customer of Secure Data; and (b) will not solicit or induce any person to leave the employ of Secure Data. Further, paragraph 2 provides that you will not divulge or use Secure Data's confidential information.

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.