THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS

CONSUMER FINANCIAL PROTECTION BUREAU, Plaintiff, v. BRIGHTSPEED SOLUTIONS, INC. and KEVIN HOWARD, Defendants.	)	Case No.

COMPLAINT

1. The Consumer Financial Protection Bureau (Bureau) brings this action against BrightSpeed Solutions, Inc. ("BrightSpeed") and Kevin Howard alleging violations of the Consumer Financial Protection Act, 12 U.S.C. §5531 and 5536(a)(1)(B), the Telemarketing and Consumer Fraud and Abuse Prevention Act (Telemarketing Act), 15 U.S.C. §§ 6101 *et seq*., and its implementing rule, the Telemarketing Sales Rule (TSR), 16 CFR § 310.3(b).

Jurisdiction and Venue

2. This Court has subject-matter jurisdiction over this action because it is brought under "Federal consumer financial law," 12 U.S.C. § 5565(a)(1), presents a federal question, 28 U.S.C. § 1331, and is brought by an agency of the United States, 28 U.S.C. § 1345.

3. Venue is proper because Defendants BrightSpeed and Howard reside in and at all relevant times transacted business in this district. 28 U.S.C. § 1391(b); 12 U.S.C. § 5564(f).

Parties

4. The Bureau is an independent agency of the United States created by the CFPA. 12 U.S.C. § 5491(a). The Bureau has independent litigating authority and is authorized to initiate civil actions in federal district court to secure appropriate relief for violations of "Federal consumer financial law," 12 U.S.C. § 5564, which includes the authority to enforce the TSR with respect to the offering or provision of a consumer financial product or service subject to the CFPA, 15 U.S.C. §§ 6102(c), 6105(d).

5. Defendant BrightSpeed was a privately owned third-party payment processor incorporated in Illinois that transacted business nationwide. BrightSpeed processed remotely created check payments (RCCs) for entities that telemarketed antivirus software and technical-support services to consumers. BrightSpeed ceased operations on or around February 2019.

6. BrightSpeed is a "covered person" under the CFPA because it "provid[ed] payments or other financial data processing services to a consumer by any technological means, including processing or storing financial or banking data for any payment instrument, or through any payment systems or network used for processing payments data." 12 U.S.C. § 5481(5). BrightSpeed offered or provided payment processing services for personal, family, or household purposes, namely for consumers who sought to obtain antivirus software and technical support services for consumers' home computers. 12 U.S.C. § 5481(5)(A). BrightSpeed is also "a person" subject to the relevant portions of the TSR. 16 C.F.R. §310.3(b).

7. Defendant Kevin Howard resides in Chicago, Illinois. He is the founder, sole owner, and chief operating officer of BrightSpeed. Howard's name appears on all state registration documents for BrightSpeed and its agreements with the banks through which it

processed payments. Howard cultivated BrightSpeed's relationships with these banks and was deeply involved in the company's day-to-day operations.

8. Howard is a "covered person" under the CFPA because he "provid[ed] payments or other financial data processing services to a consumer by any technological means, including processing or storing financial or banking data for any payment instrument, or through any payment systems or network used for processing payments data." 12 U.S.C. § 5481(5). Howard offered or provided payment processing services for personal, family, or household purposes, namely for consumers who sought to obtain antivirus software and technical-support services for their home computers. 12 U.S.C. § 5481(5)(A). Howard is a "related person" because he was the sole owner of BrightSpeed and had managerial responsibility for BrightSpeed's affairs. 12 U.S.C. § 5481(25). As a "related person," Howard is deemed a "covered person" under the CFPA. 12 U.S.C. § 5481(25)(B). Howard is also "a person" subject to the relevant portions of the TSR. 16 C.F.R. § 310.3(b).

Factual Background

Defendants' Business

9. Kevin Howard founded BrightSpeed in 2015. He served as the company's sole owner and chief operating officer from its inception through its wind-up.

10. From the outset, under Howard's leadership, BrightSpeed positioned itself as a third-party payment processor for "high-risk" telemarketing businesses. These clients, who often could not obtain payment-processing services from other payment processors because of the risk of fraud associated with their businesses, allowed Defendants to charge higher processing fees than processors with a lower risk tolerance.

11. From 2016 to 2018, Defendants BrightSpeed and Howard processed RCC payments for over 100 merchant-clients who purported to provide virus software and technical-support services, but actually scammed consumers into purchasing unnecessary and expensive computer software ("Tech-Support Clients").

12. In order to process payments for their Tech-Support Clients, Defendants opened and maintained RCC processing accounts with two regional banks ("Originating Banks").

13. Defendants maintained processing accounts at the first bank ("Bank One") from at least January 2016 to August 2018. Defendants processed over 18,000 RCC transactions for Tech-Support Clients through Bank One, totaling more than $8 million.

14. Defendants maintained processing accounts at the second bank ("Bank Two") from at least January 2016 to July 2019. Defendants processed over 150,000 RCC transactions for Tech-Support Clients through Bank Two, totaling more than $63 million.

15. Beginning in the summer of 2018, the Originating Banks terminated their relationships with the Defendants. Bank One began winding down its relationship with Defendants in August 2018 as a result of an internal investigation. Defendants then moved their remaining active merchant accounts to Bank Two, where they had an existing processing relationship. In June 2019, Bank Two also terminated its relationship with Defendants due to the excessive risk posed by their Tech-Support Clients' accounts.

Fraudulent Technical Support Scheme

16. Defendants' Tech-Support Clients typically targeted consumers using pop-up advertisements, indicating that their computers were running slowly, infected by viruses, or were experiencing some other serious technical problem. The pop-up advertisements provided consumers with a telephone number to call for assistance.

17. To appear more trustworthy, the Tech-Support Clients sometimes claimed to be affiliated with well-known technology companies like Microsoft or Symantec, but they were not affiliated with those entities.

18. If a consumer called the number, the Tech-Support Clients would typically offer services to clean or remove viruses from the consumer's computer at a steep price, sometimes as high as $2,000. When they succeeded in persuading a consumer, often an older American, to purchase their antivirus software or technical support services, Defendants' Tech-Support Clients requested payment by asking the consumer to verbally authorize an RCC and provide their name, address, bank account number, and bank routing number.

19. After obtaining authorization for payment by RCC, the Tech-Support Clients typically downloaded antivirus software, software that was sometimes available to the public for free or at a low-cost, onto the consumer's computer. These tools were frequently duplicative of software the consumer already had on his or her computer.

20. A significant number of consumers who initially authorized a transaction realized that they had been defrauded after speaking with family or friends and discovering that the software they purchased was unnecessary, ineffective, freely available, or duplicative of what they already had.

Indicia of Fraud

21. Due to their role as payment processors, Defendants knew or should have known that their Tech-Support Clients were obtaining payment for antivirus software and technical support services using RCCs. In fact, BrightSpeed's "Pre-Application Qualifying Questions," which Kevin Howard was responsible for reviewing and approving, specifically asked "what verticals do you operate in?" It also inquired about the Tech-Support Client's call center

operations. Defendants also knew that their Tech-Support Clients offered and sold these products and services over the telephone on interstate calls initiated by consumers who viewed the Tech-Support Clients' pop-up or other internet ads.

22. Defendants were also aware of nearly a thousand consumer complaints about their Tech-Support Clients. Between 2016 and 2018, Defendants received almost 1,000 consumer complaints regarding transactions that they processed, and the majority of these complaints resulted in refunds or cancellations. Approximately 25% of these complaints specifically complained that the transaction was fraudulent or unauthorized and described scenarios nearly identical to those in public service announcements published by the FBI Internet Crime Center in 2014 (available at http://www.ic3.gov/media/2014/141113.aspx) and updated in 2016 (available at http://www.ic3.gov/media/2016/160602.aspx).

23. Consumers made many of these complaints directly to Defendants. For at least 18 months, Defendants emailed transaction receipts to consumers on behalf of their Tech-Support Clients and consumers' responses came directly to Defendants. Defendants would then investigate issues consumers complained about in their responses and respond to the consumer. Further, starting around July 2016, Defendants began including BrightSpeed's phone number (instead of their clients') on the receipts so that BrightSpeed could field calls from dissatisfied customers.

24. Complaining consumers specifically mentioned the pop-up advertisements that claimed that there were problems with their computers. They complained that the Tech-Support Clients had falsely represented that they were affiliated with established companies such as Microsoft and Symantec.

25. Consumers also complained that the Tech-Support Clients created a false sense of urgency and that they were pressured and duped into purchasing unnecessary and expensive antivirus software and tech-support services from the Tech-Support Clients. Some consumers also indicated that they were contacting their local police departments or other regulatory bodies.

26. Howard and BrightSpeed also responded to inquiries from multiple police departments across the country, ranging from New York to Colorado, about police reports filed by consumers who believed they had been defrauded by BrightSpeed's Tech-Support Clients. Specifically, Howard had several conversations and exchanged emails with local police officers regarding the police reports.

Return Rates

27. A return rate is the percentage of transactions that were processed but subsequently rejected and "returned" over a given period. Transactions may be returned for a variety of reasons. For instance, a transaction may be returned due to insufficient funds in a consumer's account, invalid or closed accounts, or when a consumer explicitly rejects the transaction because he or she did not authorize it (known as "unauthorized" returns). An unauthorized return rate is a subset of the overall return rate where the reason for the return provided by the consumer is that the transaction was unauthorized.

28. The overall return rate for Defendants' Tech-Support Clients averaged between 22% and 24%. The unauthorized return rate averaged 14%.

29. By contrast, the National Automated Clearing House Association (NACHA), which manages and administers the ACH network, an analogous payment platform, has set a limit of 15% as the maximum return rate for a legitimate business and a network-wide return rate

threshold of 0.5% for unauthorized ACH transactions. NACHA's rules require network participants to report and investigate any merchant with an unauthorized return rate above 0.5%.

30. Despite the numerous indicators of fraudulent activity by their Tech-Support Clients, Defendants turned a blind eye and continued to facilitate their conduct.

Warnings from Originating Banks

31. The Originating Banks repeatedly expressed concern to Defendants about the nature and volume of the complaints that consumers lodged against the Tech-Support Clients.

32. For example, in July 2016, one of the Originating Banks contacted Defendant Howard about a complaint it received, writing:

> Kevin, it's the same story. Their customer…. received a pop-up on her computer that she had a virus with a phone number to call. When she called, they requested access to her computer, laptop, and iPad and ask[ed] for $1,200 to fix the problem. This was [Client A] again.

33. Defendants made false and misleading statements to their Originating Banks about the degree to which they vetted their Tech-Support Clients, the nature of their business relationships with their Tech-Support Clients, and the degree to which they monitored their transactions. For example:

a. Defendants told Bank One that they requested and reviewed six months of bank statements, conducted a personal credit check, criminal background check, and pulled a Dun & Bradstreet report for each potential Tech-Support Client. These representations were false.

b. Defendants told Bank Two that BrightSpeed was not a third-party payment processor in order to avoid running afoul of the bank's policy against working

with such processors and later told Bank One that it had a franchise arrangement with its Tech-Support Clients. Neither of these statements was true.

c. Defendants told Bank One that BrightSpeed called all consumers for whom it processed RCC transactions within two hours. This was not true.

d. Defendant Howard also told Bank One that he had a "personal threshold" of 4% for returns and once his clients reached that percentage, he would terminate them. This statement also was not true.

34. Defendants' false and misleading statements were meant to assuage the Originating Banks' concerns about their Tech-Support Clients' high return rates and the complaints about those clients.

Defendants' Vetting and Oversight of the Tech-Support Clients

35. Defendants failed to put reasonable controls in place to meaningfully vet their Tech-Support Clients. Defendants often did not require that the Tech-Support Clients produce documentation demonstrating that they were legitimate businesses. In some cases, Defendants only required a Tech-Support Client to complete a processing service agreement with BrightSpeed to begin processing payments for the client. In other instances, Defendants only collected generic documents, such as blank stock certificates, corporate resolutions, or a copy of the client contact's driver's license, in support of the Tech-Support Clients' applications. Defendants did not require or receive any documentation that would allow them to assess the nature of the Tech-Support Clients' businesses, the level of risk they posed to consumers, or the likelihood that they would engage in fraud.

36. Defendants also failed to monitor and promptly suspend bad actors among its Tech-Support Clients after learning that they were likely defrauding consumers or engaging in other illegal activity.

37. When a consumer complained or a bank questioned a transaction, Defendants routinely refunded the consumer. Defendants typically refunded complaining consumers' payments either by directly transmitting the funds or authorizing a return by the bank. Defendants rarely investigated the disputed transaction.

38. In some instances, in response to receiving a consumer complaint, Defendants requested and reviewed proof of authorization from the Tech-Support Client that initiated the transaction. This proof came in the form of an audio recording from the Tech-Support Client's sales call with the consumer.

39. These recordings did not encompass the entire conversation. Rather they were excerpts of the consumer reading one line of text provided by the Tech-Support Client. The text included the consumer's name, the product or service purchased, the price, the name of the Tech-Support Client, and the consumer's bank account number.

40. The recordings offered no insight into the communications that led to the sale—that is, what the consumer was told was wrong with her computer or what the products or services would accomplish; whether the Tech-Support Client claimed affiliation with companies like Microsoft or Symantec; or any other details that complaining consumers frequently mentioned.

41. Defendants continued to do business with, and earn processing fees from, Tech-Support Clients for months and sometimes years after they knew or should have known that the clients likely were engaging in fraudulent activity.

COUNT I

Violations of the Telemarketing Sales Rule and the Consumer Financial Protection Act
(*Defendants BrightSpeed and Howard*)

42. The allegations in paragraphs 1 to 41 are incorporated herein by reference.

43. Under the TSR, a "telemarketer" means any person who, in connection with telemarketing, initiates or receives telephone calls to or from a customer or donor and "telemarketing" means a plan, program, or campaign which is conducted to induce the purchase of goods or services by use of one or more telephones and which involves more than one interstate telephone call. 16 C.F.R. § 310.2(ff) and (gg).

44. It is a violation of the TSR for any seller or telemarketer to create or cause to be created, directly or indirectly, a remotely created payment order, including an RCC, as payment for goods or services offered or sold through telemarketing. 16 C.F.R. § 310.4(a)(9).

45. The TSR also prohibits a person from providing substantial assistance or support to any seller or telemarketer when that person "knows or consciously avoids knowing" that the seller or telemarketer is engaged in any act or practice that violates Section 310.4. 16 C.F.R. § 310.3(b).

46. Defendants BrightSpeed and Howard knew or consciously avoided knowing that their Tech-Support Clients were creating or causing to be created RCCs as payment for services that they offered and sold through telemarketing.

47. Despite this knowledge, Defendants BrightSpeed and Howard provided substantial assistance and support to their Tech-Support Clients by:

a. opening and maintaining processing accounts for the purpose of processing RCC payments for them;

b. processing their RCC transactions to allow them to draw funds from consumers' accounts;

c. making misrepresentations to the Originating Banks in order to prolong their ability to process RCCs for their Tech-Support Clients; and

d. failing to timely terminate their processing relationships with their Tech-Support Clients after learning of their illegal and fraudulent conduct.

48. Defendants' actions violate Section 310.3(b) of the TSR. 16 C.F.R. § 310.3(b).

49. Defendants' violations of the TSR constitute violations of the CFPA. 12 U.S.C. §§ 5531(a), 5536(a)(1); 15 U.S.C. § 6102(c)(2).

COUNT II

Unfair Acts and Practices

(*Defendants BrightSpeed and Howard*)

50. The allegations in paragraphs 1 to 41 are incorporated herein by reference.

51. Under § 1031(c)(1) of the CFPA, an act or practice is unfair when: (1) it causes or is likely to cause substantial injury to consumers; (2) which is not reasonably avoidable by consumers; and (3) such substantial injury is not outweighed by countervailing benefits to consumers or to competition.

52. Defendants' acts and practices caused substantial injury because they processed the payments of hundreds of consumers who were defrauded into purchasing unnecessary software and services. Defendants continued to process payments for their Tech-Support Clients when they knew or should have known the clients were engaged in fraud. By June 2016, Defendants also knew that their Tech-Support Clients were violating the TSR's bar on using RCCs for telemarketing transactions. Consumers also spent substantial time attempting to get refunds, including in some cases filing police reports.

53. Consumers' injuries were not reasonably avoidable because Defendants' Tech-Support Clients misled consumers about their need for software and services, the condition of their computers, and their affiliation with prominent technology companies.

54. Neither consumers nor competition experienced countervailing benefits from Defendants' processing of payments for Tech-Support Clients despite knowing, or having reason to know, that they were defrauding consumers. Processing payments for unnecessary or unauthorized services, or where the payments were obtained in an illegal manner, resulted in substantial injury that is not outweighed by countervailing benefits.

DEMAND FOR RELIEF

Wherefore, the Bureau requests that the Court:

1. prohibit Defendants from participating in any way in the business of payment processing;
2. permanently enjoin Defendants from committing future violations of the CFPA, TSR, or any provision of "Federal consumer financial law," as defined by 12 U.S.C. § 5481(14);
3. grant additional injunctive relief as the Court may deem just and proper;
4. award damages or other monetary relief against Defendants;
5. order Defendants to pay redress to consumers harmed by its unlawful conduct;
6. order Defendants to disgorge all ill-gotten gains;
7. impose on Defendants a civil money penalty;
8. order Defendants to pay the Bureau's costs and fees incurred in connection with prosecuting this action; and

9. award additional relief as the Court may determine to be just and proper.

Dated: March 3, 2021

Respectfully submitted,

Cara Petersen
Acting Enforcement Director
John C. Wells
Deputy Enforcement Director
Richa Dasgupta
Assistant Litigation Deputy

s/ Tianna Baez
Tianna Baez
(New York Bar No. 4808598)
Telephone: (202) 435-9454
Email: Tianna.Baez@cfpb.gov

Christian Woolley
(Pennsylvania Bar No. 205486)
Telephone: (202) 435-9189
Email: Christian.Woolley@cfpb.gov

1700 G Street, NW
Washington, D.C. 20552

Attorneys for Plaintiff
Consumer Financial Protection Bureau