Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of 1 the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington. 2 3 4 5 6 7 UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON 8 AT SEATTLE 9 10 NO. CR23-138 LK UNITED STATES OF AMERICA, 11 Plaintiff 12 INDICTMENT 13 V. 14 JOHN M. WHISENANT. 15 Defendant. 16 The Grand Jury charges that: 17 COUNTS 1-5 18 (Wire Fraud) 19 20 Introduction The conduct charged in this indictment victimized a private company 21 headquartered in Seattle, Washington that operated a car trade platform that allowed 22 customers to purchase, sell, and trade pre-qualified used vehicles (Company-1).1 Users 23 accessed Company-1's services through their official website or through a mobile 24 application. Company-1 was founded in 2011 and, during the time of the scheme detailed 25 26 ¹ Company - 1 has been purchased by a larger corporation and no longer operates as an independent company and the Company -1 name.

Indictment - 1 *United States v. John M. Whisenant*USAO #2022R00301

below, was staffed by fewer than 100 employees. Company-1 maintained company bank accounts at Silicon Valley Bank (SVB), based in the State of California, for its financial transactions, including sales-related payments and employee payroll, and used QuickBooks accounting software for bookkeeping.

- 2. In October 2018, Company-1 hired JOHN M. WHISENANT as a Transaction Manager. His initial duties consisted of processing the paperwork required to verify vehicle ownership and to assist customers with financing. A few months later, WHISENANT was promoted to Director of Marketplace Operations, a managerial role on the "public-facing" side of Company-1.
- 3. Approximately one year later Company-1 reduced the size of its workforce, and in so doing expanded WHISENANT's responsibilities to include managing payroll and customer sales transactions. To fulfill these tasks, Company-1 entrusted WHISENANT with unrestricted access to its payment systems. This access afforded WHISENANT the ability to send ACH (Automated Clearing House) payments from Company-1's SVB bank accounts, access to all customer transaction records, and access to its accounting records kept using QuickBooks software. WHISENANT's QuickBooks access also provided him with the QuickBooks login credentials assigned to Company-1's Chief Executive Officer (CEO). WHISENANT took advantage of this access to covertly steal over two million dollars from Company-1.
- 4. WHISENANT's employment with Company-1 ended when he abruptly resigned on February 21, 2022.

Scheme To Defraud

- 5. Beginning in or about June of 2019 and continuing through at least November 2021, in King County, within the Western District of Washington and elsewhere, JOHN M. WHISENANT, with intent to defraud, knowingly devised a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises.
- 6. The essence of this scheme and artifice to defraud was for WHISENANT to initiate numerous, unauthorized ACH transfers from Company-1's SVB bank account to

one of several, unique personal bank accounts belonging to him under his name, JOHN M. WHISENANT. It was also a part of the scheme for WHISENANT to conceal the nature of these ACH transfers by describing in their corresponding ACH bank descriptions as fictitious customer transactions or company expenses. Furthermore, unauthorized changes made by WHISENANT in Company-1's QuickBooks records that recorded these ACH transfers reflect an additional layer of concealment as part of the underlying scheme.

Manner and Means

- 7. It was part of the scheme and artifice to defraud that, while working as the Director of Marketplace Operations at Company-1, WHISENANT used his access to Company-1's SVB bank account ending in 4943 to successfully initiate, via interstate wire, at least 57 separate ACH transfers, totaling over \$2 million, from Company-1's SVB account ending in 4943 to one of 14 unique, personal bank accounts held by WHISENANT. None of the transactions were authorized.
- 8. It was further part of the scheme and artifice to defraud that the corresponding ACH descriptions for many of these transfers contained the identities of customers, many of whom had previously conducted legitimate transactions with Company-1. Other, generic ACH descriptions such as "ACH PREFUNDING" were used for the remainder of the 57 ACH transfers. These actions reflected WHISENANT's efforts to label the transactions in a way that would make them appear to be legitimate.
- 9. It was further part of the scheme and artifice to defraud that WHISENANT falsified entries in Company-1's QuickBooks records, often in conjunction with the approximate date of the fraudulent ACH transfers, to disguise these transfers as legitimate business items. Examples include receivables due from customers for made-up vehicle transactions, made-up operational expenses for purchase of vehicles from wholesalers, and reductions to payables such as sales tax payable.

Execution of Scheme and Artifice to Defraud

10. On or about the dates set forth in the table below, in King County, within the Western District of Washington, and elsewhere, WHISENANT, for the purpose of executing this scheme and artifice to defraud, did knowingly cause to be transmitted by wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, each transmission of which constitutes a separate count of this indictment:

COUNT	DATE	WIRE TRANSMISSION
1	06/18/2019	An ACH transfer in the amount of \$8,950.96 initiated from Company-1's Silicon Valley Bank account ending in 4943, which transmitted a wire and signal from outside the State of Washington to WHISENANT's Sound Credit Union account ending in 1214-10, whose servers are located in the State of Washington.
2	06/19/2019	An ACH transfer in the amount of \$13,300 initiated from Company-1's Silicon Valley Bank account ending in 4943, which transmitted a wire and signal from outside the State of Washington to WHISENANT's Sound Credit Union account ending in 1214-10, whose servers are located in the State of Washington.
3	07/15/2019	An ACH transfer in the amount of \$10,001 initiated from Company-1's Silicon Valley Bank account ending in 4943, which transmitted a wire and signal from outside the State of Washington to WHISENANT's Sound Credit Union account ending in 1214-10, whose servers are located in the State of Washington.
4	09/04/2019	An ACH transfer in the amount of \$20,372 initiated from Company-1's Silicon Valley Bank account ending in 4943, which transmitted a wire and signal from outside the State of Washington to WHISENANT's Sound Credit Union account ending in 1214-10, whose servers are located in the State of Washington.
5	01/16/2020	An ACH transfer in the amount of \$11,539.47 initiated from Company-1's Silicon Valley Bank account ending in 4943, which transmitted a wire and signal from outside the State of Washington to WHISENANT's Sound Credit Union account ending in 8959, whose servers are located in the State of Washington.

All in violation of Title 18, United States Code Section 1343.

Indictment - 5 *United States v. John M. Whisenant*USAO #2022R00301

ASSET FORFEITURE ALLEGATION

1. The allegations contained in Counts 1 – 5 of this Indictment are hereby realleged and incorporated by reference for the purpose of alleging forfeiture. Upon conviction of any of the offenses alleged in Counts 1 - 5, JOHN M. WHISENANT shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C), by way of Title 28, United States Code, Section 2461(c), all property constituting or traceable to proceeds of the wire-fraud scheme described above, including but not limited to a judgment for a sum of money in the amount of \$2,084,799.08 reflecting the proceeds Defendant obtained as a result of the scheme.