MELISSA HOLYOAK, United States Attorney (#9832)
MARK E. WOOLF, Assistant United States Attorney (WA #39399)
LUISA GOUGH, Assistant United States Attorney (#17221)
Attorneys for the United States of America
Office of the United States Attorney
111 South Main Street, Suite 1800
Salt Lake City, Utah 84111-2176
Telephone: (801) 524-5682

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH

UNITED STATES OF AMERICA,

Plaintiff,

vs.

JONATHAN REMBERT,

Defendant.

INDICTMENT

Count 1: Conspiracy to Commit Wire Fraud, 18 U.S.C. §§ 1349 and 1343

Count 2: Conspiracy to Commit Mail Fraud, 18 U.S.C. §§ 1349 and 1341

Count 3: Possession of Fifteen or More Unauthorized Access Devices, 18 U.S.C. § 1029(a)(3)

Counts 4-9: Aggravated Identity Theft, 18 U.S.C. § 1028A

The Grand Jury Charges:

1. Defendant **JONATHAN REMBERT** ("**REMBERT**") is a resident of Fort Mill, South Carolina.

I. The Scheme and Conspiracy to Defraud

2. Beginning on a date unknown, but not later than November 2020, and continuing through at least May 2024, within the District of Utah and elsewhere, **REMBERT**, acting independently and interdependently with others known and unknown to the Grand Jury, combined, conspired, and agreed to devise and execute a scheme and artifice to defraud in order to obtain money or property by means of false or fraudulent pretenses, representations, or promises, and omissions of material facts through the unauthorized sale of "discounted" ski and snowboard passes, including IKON passes, EPIC passes, and individual resort passes.

3. The EPIC Pass is a mountain resort access pass sold by Vail Resorts, Inc. ("Vail Resorts"), a Colorado based company. Vail Resorts is a global company that owns and operates forty-two mountain resorts throughout the world, including Park City Mountain Resort, in Park City, Utah. Vail Resorts partners with other mountain resorts to provide additional access to purchasers of the EPIC Pass.

4. The IKON Pass is a mountain resort access pass sold by Alterra Mountain Company ("Alterra"), which is a conglomerate of several mountain resorts with its corporate headquarters in Colorado. Alterra is the parent company of Solitude Mountain Resort and Deer Valley Resort, which are both located within the District of Utah. The IKON Pass sold by Alterra offers purchasers access to the following Utah resorts: Alta Ski Area, Brighton Resort, Deer Valley Resort, Snowbasin Resort, Snowbird, and

Solitude Mountain Resort. The IKON Pass also provides purchasers access to additional mountain resorts throughout the United States and world.

II. Object of the Scheme and Conspiracy

5. It was the object of the scheme and conspiracy for **REMBERT**, acting alone and in combination, agreement, and interdependently with others known and unknown to the Grand Jury, to obtain money from individual purchasers ("Pass Purchasers") through the unauthorized sale of "discount" ski and snowboard passes, including the IKON Pass, the EPIC Pass, and individual mountain resort passes.

III. Manner and Means of the Scheme and Conspiracy

6. It was the manner and means of carrying out the scheme and conspiracy that **REMBERT**, within the District of Utah and elsewhere, acting alone and interdependently in combination and agreement with others known and unknown to the Grand Jury, would:

a. place targeted online advertisements, within the District of Utah and elsewhere, offering "discounted" ski and snowboard passes to Pass Purchasers.

b. communicate directly with Pass Purchasers who responded to the online advertisements, or, in some instances, were prior customers and/or referred by others, through text and other forms of electronic and telephonic communication.

c. falsely claim they were authorized to sell heavily discounted ski and snowboard passes, including the IKON Pass and EPIC Pass.

d. obtain personal information from Pass Purchasers, including names, addresses, email addresses, dates of birth, and, in some instances, login information for previously existing accounts held in the names of Pass Purchasers at mountain resorts, including Alterra (IKON Pass) and Vail Resorts (EPIC Pass).

e. confirm to Pass Purchasers the ability to sell "discount" ski and snowboard passes to Pass Purchasers, including the IKON Pass and EPIC Pass, and, in most instances, establish with Pass Purchasers an agreed "discount" price for whatever ski and snowboard pass the Pass Purchasers sought to purchase.

f. use the Pass Purchasers' personal information, prior to obtaining payment of the "discount" price from Pass Purchasers, to establish new accounts for the Pass Purchasers or access previously existing accounts held by the Pass Purchasers using the online portals of individual resorts, Alterra (IKON Pass), and Vail Resorts (EPIC Pass).

g. purchase, once online accounts had been established and accessed for the Pass Purchasers, ski and snowboard passes for the Pass Purchasers at *full price* using stolen bank card information. The stolen bank card information

used to make the *full price* purchases of ski and snowboard passes was obtained and shared between **REMBERT**, and others known and unknown to the Grand Jury, prior to the *full price* purchases being made and without the knowledge of the Pass Purchasers. The *full price* purchases made with the stolen bank card information resulted in the ski and snowboard passes purchased on behalf of Pass Purchasers being delivered to the Pass Purchasers electronically and, in some instances, via the United States Postal Service.

h. resume communication, after purchasing the ski and snowboard passes for *full price* using stolen bank card information, with the Pass Purchasers to confirm the purchases and, to the extent a "discount" price had not already been negotiated, negotiate a "discounted" price for payment by the Pass Purchasers and demand payment through peer-to-peer ("P2P") applications.

i. receive Pass Purchasers' payments through agreed P2P applications, including, without limitation, Venmo, PayPal, Zelle, and Apple Pay, said funds being deposited directly into accounts held and controlled by **REMBERT** and others known and unknown to the Grand Jury.

j. divert and disseminate those proceeds amongst themselves for personal use.

7. The scheme and conspiracy included, among others, conduct against the following Pass Purchasers, among others:

a. Pass Purchaser AW ("AW"):

i. On or about October 23, 2022, AW messaged telephone number xxx-xxx-4695 to purchase a "discounted" IKON Pass via an interstate wire communication. AW provided the following information: name, date of birth, email address, and a mailing address in Salt Lake City, Utah.

ii. On or about October 31, 2022, an IKON Pass was purchased in AW's name using stolen bank card information with a billing address in Charlotte, North Carolina.

iii. Alterra sent the IKON Pass to AW by U.S. Mail to an address in Salt Lake City, Utah.

iv. On or about October 31, 2022, AW received confirmation of the purchased IKON Pass and instructions to send funds representing the "discounted" price of the IKON Pass via Venmo to username @xxxxx. On or about December 16, 2022, AW sent $580, via an interstate wire communication, through Venmo as instructed.

v. The purchase of AW's IKON Pass using stolen bank card information was reported as fraudulent, resulting in a charge back to Alterra and revocation of AW's IKON Pass.

b. Pass Purchaser JW ("JW"):

i. On or about October 18, 2023, JW messaged telephone number xxx-xxx-6779 to purchase a "discounted" IKON Pass via an interstate wire communication. JW provided the following information: name, date of birth, email address, and a mailing address in West Jordan, Utah.

ii. On or about November 13, 2023, an IKON Pass was purchased in JW's name using stolen bank card information with a billing address in Spokane, Washington.

iii. On or about November 13, 2023, JW received confirmation that the IKON Pass was purchased in JW's name and a request to send funds representing the "discounted" price of the IKON Pass via Venmo to username @xxxxx. On or about November 14, 2023,

J.W. sent $580, via an interstate wire communication, through Venmo as instructed.

iv. The purchase of JW's IKON Pass using stolen bank card information was reported as fraudulent, resulting in a charge back to Alterra and revocation of JW's IKON Pass.

c. Pass Purchaser SM ("SM"):

i. On or about November 30, 2023, SM messaged telephone number xxx-xxx-4695 to purchase a "discounted" season pass to Alta Ski Area, a Utah ski resort, via interstate wire communication. SM provided the following information: name, date of birth, email address, and a mailing address in Salt Lake City, Utah.

ii. On or about December 1, 2023, a season pass to Alta Ski Area was purchased in SM's name using stolen bank card information with a billing address in Corvallis, Oregon.

iii. On or about December 1, 2023, SM received confirmation of the purchase of a season pass for Alta Ski Area season pass and a demand to send funds representing the "discounted" price of the season pass to Venmo to username @xxxxx. On or about December 1, 2023, SM sent $595, via interstate wire communication, through Venmo as instructed.

iv. The purchase of the Alta Ski Area with stolen bank card information was reported as fraudulent, resulting in a charge back to Alta Ski Area.

d. Pass Purchaser RB ("RB"):

i. On or about February 17, 2023, RB, a resident of Utah, messaged Facebook user "xxxxx xxxxx," and later telephone number xxx-xxx-2589, to purchase a "discounted" day pass to Breckenridge Ski Resort, which is located in Colorado and owned by Vail Resorts, through interstate wire communication. RB provided the following information: name, date of birth, and an email address.

ii. On or about February 25, 2023, a day pass to Breckenridge Ski Resort was purchased in RB's name using stolen bank card information with a billing address in Crowley, Texas.

iii. On or about February 25, 2023, RB received confirmation of the day pass purchase and instruction to send funds representing the "discounted" price via Venmo to username @xxxxx. RB sent $115.00, via interstate wire communication, through Venmo as instructed.

iv. The purchase of RB's day pass with stolen bank card information was reported as fraudulent, resulting in a charge back to Vail Resorts.

e. Pass Purchaser KT ("KT"):

i. On or about September 29, 2022, KT messaged telephone number xxx-xxx-2589 to purchase a "discounted" IKON Pass via interstate wire communication. KT provided the following information: name, date of birth, email address, and a mailing address in Salt Lake City, Utah.

ii. On or about October 12, 2022, an IKON Pass was purchased in KT's name using stolen bank card information with a billing address in Hiawassee, Georgia.

iii. Alterra sent the IKON Pass to KT by U.S. Mail to an address in Salt Lake City, Utah.

iv. On or about October 13, 2022, KT sent $580.00, via interstate wire communication, representing the "discounted" IKON Pass price via PayPal to username xxxxx@icloud.com, as previously instructed during interstate wire communications with the xxx-xxx-2589 telephone number.

v. The purchase of KT's IKON Pass using stolen bank card information was reported as fraudulent, resulting in a charge back to Alterra and revocation of KT's IKON Pass.

f. Pass Purchaser AW2 ("AW2"):

i. On or about September 17, 2022, AW2 messaged telephone number xxx-xxx-2589 to purchase "discounted" IKON Passes via interstate wire communication. AW2 provided the following information: name, date of birth, email address, and a mailing address in Holladay, Utah.

ii. On or about September 22, 2022, multiple IKON Passes were purchased on behalf of AW2 using stolen bank card information with a billing address in Madison, Alabama.

iii. Alterra sent the IKON Passes to AW2 using by Alterra via U.S. Mail to an address in Holladay, Utah.

iv. On or about September 22, 2022, AW2 received confirmation of the IKON Passes purchase and was instructed to send funds representing the "discounted" price for the IKON Passes via PayPal to xxxxx@icloud.com. AW2 sent $1,160.00, via interstate wire communication, through PayPal as instructed.

v. The purchase of AW2 IKON Pass using stolen bank card information was reported as fraudulent, resulting in a charge back to Alterra and revocation of AW2's IKON Pass.

g. Pass Purchaser WM ("WM"):

i. On or about May 11, 2023, WM messaged telephone number xxx-xxx-4695 to purchase "discounted" season passes to Alta Ski Area, a Utah ski resort, via interstate wire communication. WM provided the following information: name, date of birth, email address, and a mailing address in Cottonwood Heights, Utah.

ii. On or May 18, 2023, multiple Alta Ski Area season passes were purchased on behalf of WM using stolen bank card information with a billing address in De Pere, Wisconsin.

iii. On or about May 19, 2023, as previously instructed in text communications with telephone number xxx-xxx-4695, WM sent $1,431.70, via interstate wire communication, through Venmo to

username @xxxxx, said funds representing the "discounted" price for the Alta Ski Area season passes.

iv. The purchase of the Alta Ski Area passes using stolen bank card information was reported as fraudulent, resulting in a charge back to Alta Ski Area and revocation of WM's passes.

h. Pass Purchaser ST ("ST"):

i. On or about September 30, 2021, ST messaged telephone number xxx-xxx-4695 to purchase a "discounted" EPIC Pass via interstate wire communication. ST provided the following information: name, date of birth, email address, and a mailing address in Denver, Colorado.

ii. On or about September 30, 2021, an EPIC Pass was purchased in ST's name using stolen bank card information with a billing address in Benton, Arkansas.

iii. On or about September 30, 2021, in text communications with telephone number xxx-xxx-4695, ST was provided a confirmation number for the EPIC Pass purchase and instructions to send the "discounted" price for the EPIC Pass to PayPal user xxxxx@icloud.com. On or about October 1, 2021, ST sent $300, via interstate wire communication, through PayPal user xxxxx@icloud.com as instructed.

iv. The purchase of ST's EPIC Pass using stolen bank card information was reported as fraudulent, resulting in a charge back to Vail Resorts.

i. Pass Purchaser JV ("JV"):

i. On or about August 30, 2023, JV messaged telephone number xxx-xxx-4695 to purchase a "discounted" EPIC Pass via interstate wire communication. JV provided the following information: name, date of birth, email address, and a mailing address in Massapequa, New York.

ii. On or about August 30, 2023, an EPIC Pass was purchased in JV's name using stolen bank card information with a billing address in Heber City, Utah.

iii. On or about August 30, 2023, in text communications with telephone number xxx-xxx-4695, JV was provided a confirmation number for the EPIC Pass purchase and instructions to send the "discounted" price for the EPIC Pass to Venmo user @xxxxx, and, on or about August 30, 2023, JV did as instructed and sent $450.00, via interstate wire communication, through Venmo user @xxxxx.

i. The purchase of JV's EPIC Pass using stolen bank card information was reported as fraudulent, resulting in a charge back to Vail Resorts and revocation of JV's EPIC Pass.

8. The scheme and conspiracy resulted in millions of dollars of loss. Many individuals whose stolen bank card information REMBERT and his confederates used without the individuals' knowledge or authorization challenged the pass purchase transactions as fraudulent, resulting in large scale "charge backs" borne by the various mountain resorts, including Alterra and Vail Resorts, when the funds were returned to the bank card holders. Many of the ski and snowboard passes obtained by Pass Purchasers were cancelled as a result of the charge backs and the fraud.

COUNT 1
18 U.S.C. §§ 1349
(Conspiracy to Commit Wire Fraud)

9. All factual allegations set forth above are incorporated herein by reference.

10. Beginning on a date unknown, but not later than November 2020, and continuing through at least May 2024, within the District of Utah and elsewhere,

JONATHAN REMBERT,

defendant herein, and others known and unknown to the Grand Jury, intentionally combined, conspired, and agreed with each other to commit an offense under 18 U.S.C. § 1343 (Wire Fraud), that is, to knowingly devise or intend to devise a scheme and artifice to defraud in order to obtain money or property by means of false and fraudulent pretenses, representations, promises, and omissions of material facts.

11. It was a part of the conspiracy that **REMBERT** and his coconspirators would engage in the conduct described in parts a through j of paragraph 6 above,

all in violation of 18 U.S.C. §§ 1349.

COUNT 2
18 U.S.C. §§ 1349
(Conspiracy to Commit Mail Fraud)

12. All factual allegations set forth above are incorporated herein by reference.

13. Beginning on a date unknown, but not later than November 2020, and continuing through at least May 2024, within the District of Utah and elsewhere,

JONATHAN REMBERT,

defendant herein, and others known and unknown to the Grand Jury, intentionally combined, conspired, and agreed with each other to commit an offense under 18 U.S.C. § 1341 (Mail Fraud), that is, to knowingly devise or intend to devise a scheme and artifice to defraud in order to obtain money or property by means of false or fraudulent pretenses, representations, or promises and for the purpose of executing such scheme or

artifice or attempting to do so, place in any post office or authorized depository for mail matter, any matter or thing whatever to be sent or delivered by the Postal Service, or deposits or causes to be deposited any matter or thing whatever to be sent or delivered by any private or commercial interstate carrier, or takes or receives therefrom, any such matter or thing, or knowingly causes to be delivered by mail or such carrier according to the direction thereon, or at the place at which it is directed to be delivered by the person to whom it is addressed, any such matter or thing.

14. It was a part of the conspiracy that **REMBERT** and his coconspirators would engage in the conduct described in parts a through j of paragraph 6 above, all in violation of 18 U.S.C. §§ 1349.

COUNT 3
18 U.S.C. § 1029(a)(3)
(Possession of 15 or More Unauthorized Access Devices)

15. All factual allegations set forth above are incorporated herein by reference.

16. On or about January 20, 2023, within the District of Utah and elsewhere,

JONATHAN REMBERT,

defendant herein, did knowingly and with the intent to defraud, possess at least fifteen or more unauthorized access devices, as defined in 18 U.S.C. § 1029(e)(1) and 18 U.S.C. § 1029(e)(3), with said possession affecting interstate and foreign commerce in violation of 18 U.S.C. § 1029(a)(3). One of the unauthorized access devices unlawfully possessed

by **REMBERT** belonged to a resident of Utah and was used, without lawful authority, multiple times during the scheme and conspiracy resulting in financial loss.

COUNTS 4-9
18 U.S.C. § 1028A
(Aggravated Identity Theft)

17. All factual allegations set forth above are incorporated herein by reference.

18. On or about the dates alleged below, in the District of Utah, and elsewhere,

JONATHAN REMBERT,

defendant herein, did knowingly transfer, possess, or use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, conspiracy to commit wire fraud in violation of 18 U.S.C. §§ 1349, as well as conspiracy to commit mail fraud, in violation of 18 U.S.C. §§ 1349, each transfer, possession, or use described below constituting a separate count, all in violation of 18 U.S.C. § 1028A:

COUNT	TRANSFER, POSSESSION, USE	SKI PASS PURCHASER
4	Transfer, possession, or use of a means of identification of victim ES, a true and living person in Benton, Arkansas	ST, *see* ¶ 7(h)
5	Transfer, possession, or use of a means of identification of victim KC, a true and living person in Charlotte, North Carolina	AW, *see* ¶ 7(a)
6	Transfer, possession, or use of a means of identification of victim SC, a true and living person in Crowley, Texas	RB, *see* ¶ 7(d)
7	Transfer, possession, or use of a means of identification of victim PS, a true and living person in De Pere, Wisconsin	WM, *see* ¶ 7(g)

8	Transfer, possession, or use of a means of identification of victim RM, a true and living person in Heber City, Utah	JV, *see* ¶ 7(i)
9	Transfer, possession, or use of a means of identification of victim DR, a true and living person in Spokane, Washington	JW, *see* ¶ 7(b)

NOTICE OF INTENT TO SEEK FORFEITURE

Pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), upon conviction of any offense violating 18 U.S.C. §§ 1341, 1343, and/or 1349, the defendant shall forfeit to the United States of America any property, real or personal, that constitutes or is derived from proceeds traceable to the scheme to defraud.

The United States may seek a forfeiture money judgement and may seek to forfeiture substitute assets under 21 U.S.C. § 853(p).

A TRUE BILL:

/s/
FOREPERSON OF GRAND JURY

MELISSA HOLYOAK
United States Attorney

Mark E. Woolf
MARK E. WOOLF
LUISA GOUGH
Assistant United States Attorneys