Trials@uspto.gov
571-272-7882

Paper No. 7
Entered: July 12, 2019

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

UNIFIED PATENTS, INC.
Petitioner,

v.

SECUREWAVE STORAGE SOLUTIONS, INC.,
Patent Owner.

Case IPR2019-00501
Patent 7,036,020

Before JONI Y. CHANG, ANNETTE R. REIMERS, and GARTH D. BAER, *Administrative Patent Judges*.

BAER, *Administrative Patent Judge*.

DECISION
Instituting *Inter Partes* Review
37 C.F.R. § 42.108

I. INTRODUCTION

Unified Patents Inc. ("Petitioner") filed a Petition (Paper 2, "Pet."), requesting an *inter partes* review of claims 1–5 (the "challenged claims") of U.S. Patent No. 7,036,020 (Ex. 1001, "the '020 patent"). SecureWave Storage Solutions, Inc. ("Patent Owner") filed a Preliminary Response to the Petition (Paper 6, "Prelim. Resp.").

Pursuant to 35 U.S.C. § 314(a), an *inter partes* review may not be instituted unless "the information presented in the petition . . . shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition." Having considered the Petition and the Preliminary Response, we determine that there is a reasonable likelihood that Petitioner would prevail in establishing that claims 1–5 of the '020 patent are unpatentable. Therefore, for the reasons set forth below, we institute an *inter partes* review of claims 1–5.

A. RELATED PROCEEDINGS

The parties identify *SecureWave Storage Solutions, Inc. v. Kingston Tech. Co., Inc.*, Case No. 8:18-cv-01425 (C.D. Cal.) and *SecureWave Storage Solutions, Inc. v. Micron Tech., Inc.*, Case No. 18-cv-01398-MN (D. Del.) as related matters. Paper 4, 2–3. The parties also note that the '020 patent is at issue in IPR2019-00494. *Id.* at 2.

B. THE '020 PATENT

The '020 patent is directed to a storage device in a computer system. Ex. 1001, Abstract. The storage device includes a security partition with restricted access. *Id.* The storage device further includes at least one authority record and associated data. *Id.* The methods and systems in the '020 patent promote security in the computer system. *Id*.

C. ILLUSTRATIVE CLAIM

Petitioner challenges claims 1–5 of the '020 patent. Claim 1 is the only independent challenged claim and is reproduced below:

> 1. A storage device for promoting security in a computer system, the storage device comprising:
>
> a storage medium for storing data;
>
> firmware for reading data from and writing data two the storage medium; and
>
> a partition defined on the storage medium for dividing the storage medium into a data partition and a secure data partition, the secure data partition for storing secure data and one or more authority records, wherein the one or more authority records define access permissions relating to the secure data partition and the secure data;
>
> wherein the secure data partition contains a master authority record, wherein the one or more authority records can be created and deleted as required by a user having access permissions according to the master authority record; and
>
> wherein only the firmware is permitted to access the secure data and the one or more authority records.

Ex. 1001, 12:52–13:2.

D. Asserted Grounds of Unpatentability

Petitioner asserts the following grounds of unpatentability. Pet. 9.

References	Basis	Challenged Claims
Guthery[1] and Dethloff[2]	§ 103	1–5
Guthery, Dethloff, and Moran[3]	§ 103	1–5
Robb[4], Jones[5], and Grawrock[6]	§ 103	1–5

II. ANALYSIS

A. Discretion to Deny Institution

Patent Owner asserts that the Petition's three asserted grounds address the same claims without explaining the relative strengths of each asserted ground. Prelim. Resp. 16. According to Patent Owner, "the Board should require the Petitioner to elect only one ground between Grounds 1, 2, and 3, and deny institution on the unelected grounds." *Id*. We do not have authority to require Petitioner to select one ground and deny institution on the unelected grounds. *See BioDelivery Sci. Int'l, Inc. v. Aquestive Therapeutics, Inc.*, 898 F.3d 1205, 1209 (Fed. Cir. 2018) (holding that *SAS Institute, Inc. v. Iancu*, 138 S.Ct. 1348 (2018) "requires institution on all challenged claims and all challenged grounds").

B. Claim Construction

Petitioner proposes constructions for "authority record" and "master authority record." Pet. 10–12. According to Petitioner, "the phrase 'one or

[1] U.S. Patent No. 6,567,915 B1 (filed October 23, 1998) (Ex. 1004).
[2] U.S. Patent No. 4,837,422 (issued June 6, 1989) (Ex. 1005).
[3] U.S. Patent No. 6,324,537 B1 (filed September 30, 1999) (Ex. 1006).
[4] U.S. Patent No. 6,931,503 B1 (PCT entered national phase November 7, 2000) (Ex. 1007).
[5] U.S. Patent No. 5,623,637 A (issued April 22, 1997) (Ex. 1008).
[6] U.S. Patent No. 6,081,893 A (issued June 27, 2000) (Ex. 1009).

more authority records' means 'at least one record that defines who or what has access to the secure partition and secure data'" and "[t]he phrase 'master authority record' means 'an authority record that provides access permissions for a user to create or delete other authority records.'" *Id.* at 10.

Patent Owner asserts these constructions are too narrow given their context within the claims. Prelim. Resp. 17–21. However, even if Patent Owner is correct, Petitioner's constructions are enough to determine whether to institute *inter partes* review. Petitioner may meet its burden to show that the cited prior art teaches or suggests those limitations according to its narrow constructions. Based on the current record, we construe "one or more authority records" to include at least one record that defines who or what has access to the secure partition and secure data. We construe "master authority record" to include an authority record that provides access permissions for a user to create or delete other authority records. We decline to resolve whether Petitioner's constructions are too narrow. *See Vivid-Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999) ("[O]nly those terms need be construed that are in controversy, and *only to the extent necessary to resolve the controversy*.") (emphasis added).

C. ASSERTED PRIOR ART

1. Guthery (Ex. 1004)

Guthery discloses an integrated circuit device such as a "smart" credit or debit card for authenticating identities and authorizing transactions. Ex. 1004, Abstract. An exemplary smart card implementation of this device includes an EEPROM 58 that stores data, and a ROM 56 that includes cryptographic and other programs for performing its functions. *Id.* at 6:26–50. Figure 2 is reproduced below.

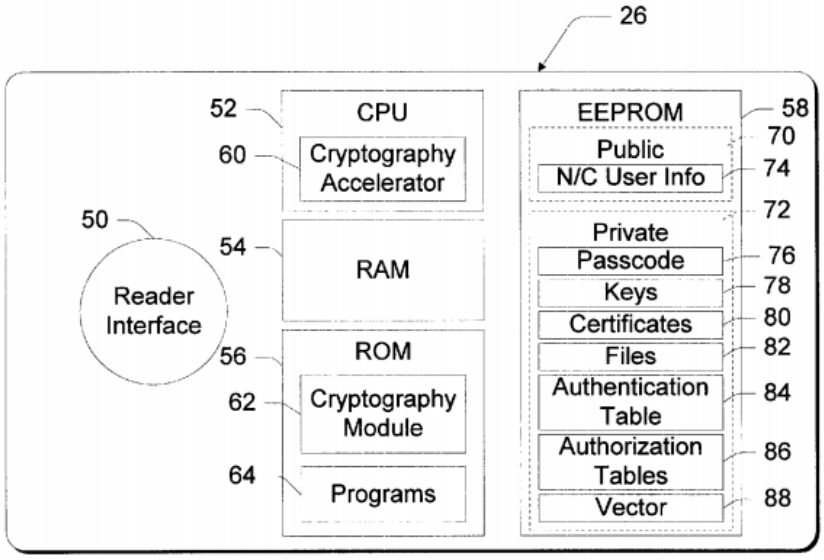

Fig. 2

Figure 2 illustrates this smart card implementation. *Id.* at 6:12–13.

2. Dethloff (Ex. 1005)

Dethloff discloses a system for programming smart cards containing integrated circuits. Ex. 1005, Abstract, 1:12–20. A cardholder uses a master enabling code to allow access for programming the cards for subordinate user accounts. *Id*. at Abstract.

3. Moran (Ex. 1006)

Moran discloses a system for controlling access to data stored in an electronic storage device. Ex. 1006, Abstract. Figure 1 is reproduced below.

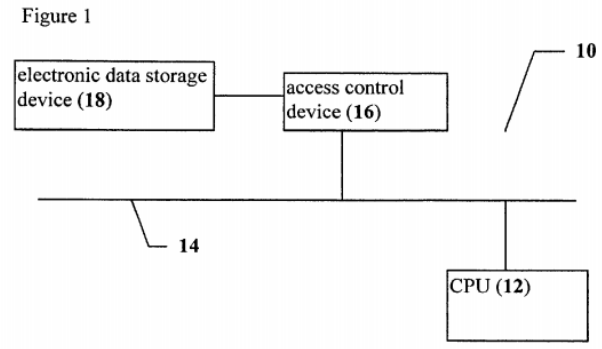

Figure 1 illustrates a schematic diagram of this system. *Id.* at 2:24–25. In this system, "any attempts to access data in data storage device 18 must pass through access control device 16." *Id.* at 5:35–38.

4. Robb (Ex. 1007)

Robb discloses a storage device including a storage medium for storing information, and a ROM for storing firmware for controlling operation of the storage device. Ex. 1007, Abstract. The firmware stored in ROM includes a supervisor that protects information stored on the storage medium. *Id.* Figure 1 is reproduced below.

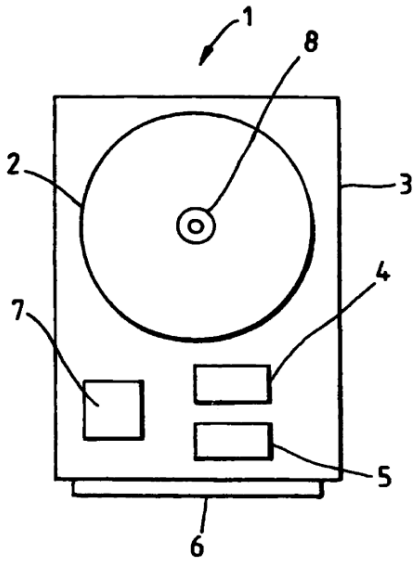

Fig. 1

Figure 1 illustrates a hard disk drive embodiment. *Id.* at 7:9–10.

5. Jones (Ex. 1008)

Jones discloses:

> [a] detachable PCMCIA memory card incorporating a smart-card integrated circuit for storing a password value and logic circuitry for preventing access to information stored on the memory card unless the user of the host computer to which the memory card is connected can supply a password matching the stored password.

Ex. 1008, Abstract. Figure 1 is reproduced below.

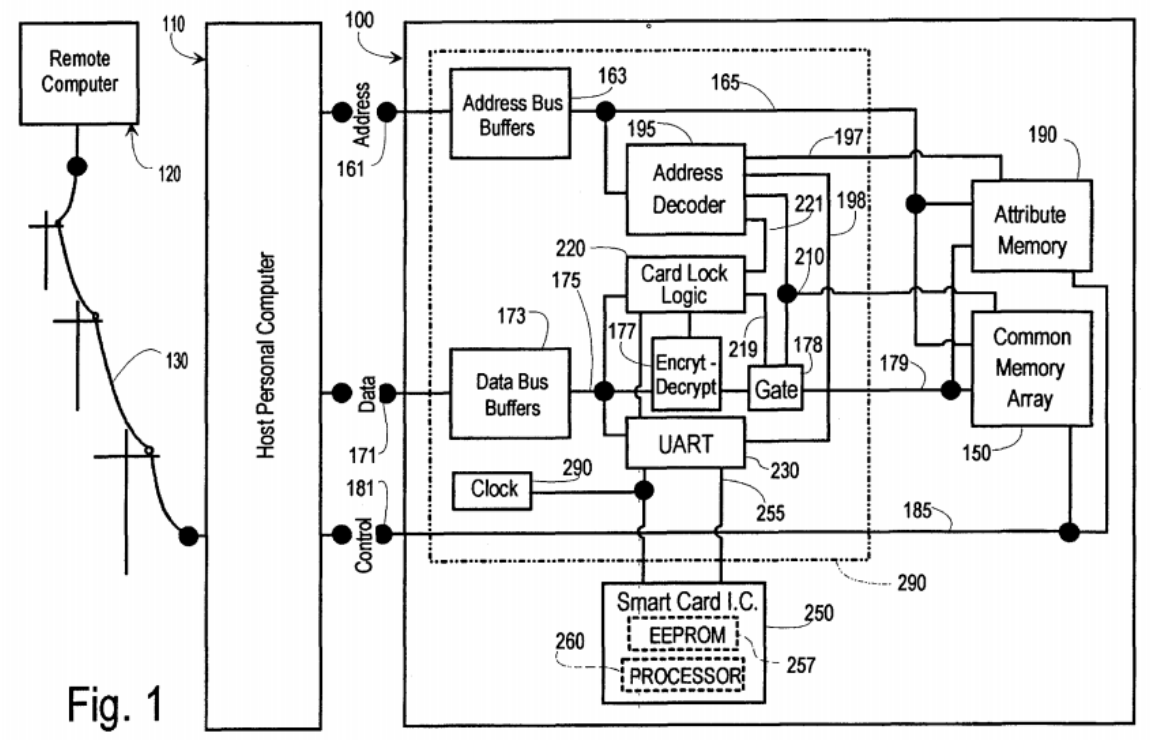

Fig. 1

Figure 1 illustrates a block diagram of the secure memory card. *Id.* at 2:66–67. This card includes common memory array 150 that stores data, *id.* at 3:50–55, non-volatile attribute memory 190 that establishes an interface with the host computer, *id.* at 4:23–30, and smartcard IC 250 that stores and controls access for secret keys, *id.* at 5:1–7.

6. Grawrock (Ex. 1009)

Grawrock discloses a password-based system for controlling access to secure files in a workstation. Ex. 1009, Abstract. A system administrator is authorized to create their own password and default log-in records for further authorized users, who in turn provide their own new passwords. *Id.* at 15:43–61.

D. OBVIOUSNESS ANALYSIS

1. First Ground: Obviousness of Claims 1–5 based on Guthery and Dethloff

Petitioner asserts that independent claim 1 is obvious over Guthery and Dethloff. Pet. 18. For the reasons explained below, we find that Petitioner has not made an adequate showing that this combination of references discloses or make obvious the limitations "firmware for reading data from and writing data to the storage medium" and "one or more authority records." Despite these deficiencies, we include this ground in the instituted trial. *See BioDelivery Sci. Int'l, Inc. v. Aquestive Therapeutics, Inc.*, 898 F.3d 1205, 1209 (holding that *SAS Institute, Inc. v. Iancu*, 138 S.Ct. 1348 (2018) "requires institution on all challenged claims and all challenged grounds").

a. "firmware for reading data from and writing data to the storage medium"

Claim 1 requires "firmware for reading data from and writing data to the storage medium." Petitioner relies on Guthery for this limitation. Pet. 20–21. Specifically, Petitioner asserts Guthery's cryptographic program 62 and one or other programs 64 disclosing claim 1's firmware for reading data from and writing data to the storage medium. *Id.* at 20. We disagree. In particular, Petitioner has not sufficiently demonstrated that any of Guthery's "cryptographic functions" performed by cryptographic program 62 are used in reading from and writing to the EEPROM 58 (i.e., the storage medium). *See* Ex. 1004, 6:25–40. Also, we do not find Petitioner's assertion that the use of programs 64 "to facilitate sessions with corresponding programs on the point-of-transaction unit 22," *id*. at 6:40–43, means that these programs are for reading data from and writing data to EEPROM 58, as claim 1 requires. *See* Pet. 20. While reading and writing data may occur within

sessions, we agree with Patent Owner that facilitating sessions with outside programs does not necessarily involve the firmware reading from and writing to the storage medium. *See* Prelim. Resp. 23–24. In addition, although Guthery elsewhere describes writing data to the storage device (i.e., "by explaining that '[i]dentities may be added to and removed from the card by simply altering' the authentication table," Pet. 20–21 (quoting Ex. 1004, 7:66–8:2)), Guthery does not indicate that the storage device's firmware performs those functions. Instead, as Patent Owner points out, "Guthery merely states that the adding and removal of identities can occur." Prelim. Resp. 26.

b. "access permissions according to the master authority record"

Claim 1 recites "a master authority record, wherein the one or more authority records can be created and deleted as required by the user having access permissions according to the master authority record." Petitioner asserts that Dethloff discloses this limitation. Pet. 26, 28. Specifically, Petitioner relies on Dethloff's cardholder's PIN 210 as a "master enabling code" used "to authenticate a particular user with the rights to add and delete identities in Guthery's smart card authentication table 84." *Id.* at 27. We do not agree that Dethloff's cardholder's PIN is a master authority record. Although Dethloff's cardholder has authority to open sub-user accounts, Ex. 1005, Abstract, Dethloff does not disclose that the cardholder's PIN indicates this authority as the claim limitation requires under Petitioner's proffered construction. That is, a PIN, by itself, does not disclose "access permissions according to the master authority record" because, while a PIN is information used to authenticate a user, the PIN does not have information about what access an authenticated user has. Thus, we agree with Patent

Owner that Dethloff's PIN does not disclose a master authority record, as claimed. *See* Prelim. Resp. 35–36.

Given the deficiencies outlined above, we find that Petitioner has not shown sufficiently that claim 1 is obvious over its proffered combination of Guthery and Dethloff. Claims 2–5 depend ultimately from claim 1. None of Petitioner's analysis for claims 2–5 remedy the deficiencies explained above related to claim 1. Therefore, on this record and for the purposes of this Decision, Petitioner has not shown a reasonable likelihood that it would prevail in establishing claims 1–5 would have been obvious over Guthery and Dethloff.

2. Second Ground: Obviousness of Claims 1–5 based on Guthery, Dethloff, and Moran

Petitioner asserts that independent claims 1–5 are obvious over a combination of Guthery, Dethloff, and Moran. Pet. 34. This ground parallels Ground 1, except that Petitioner adds Moran to account for the firmware limitations. Pet. 36–38. Petitioner, however, still relies on Dethloff for disclosing claim 1's master authority record. *Id.* at 35. Because Moran does not remedy the deficiency explained above with respect to the claimed master authority record, on this record and for the purposes of this Decision, Petitioner has not shown a reasonably likelihood that it would prevail in establishing claims 1–5 would have been obvious over Guthery, Dethloff, and Moran. Despite its deficiencies, we include this ground in the instituted trial. *See BioDelivery Sci. Int'l, Inc. v. Aquestive Therapeutics, Inc.*, 898 F.3d 1205, 1209 (holding that *SAS Institute, Inc. v. Iancu*, 138 S.Ct. 1348 (2018) "requires institution on all challenged claims and all challenged grounds").

3. Third Ground: Obviousness of Claims 1–5 based on Robb, Jones, and Grawrock

Petitioner asserts that independent claims 1–5 are obvious over a combination of Robb, Jones, and Grawrock. Pet. 42. Based on Petitioner's analysis and as explained below, we find Petitioner has made an adequate showing that claims 1–5 would have been obvious over Robb, Jones, and Grawrock.

a. Petitioner's Proffered Combination

Petitioner cites Robb as disclosing claims 1's preamble, storage medium, firmware, and partition. Pet. 47–49, 55. Petitioner asserts that Jones discloses the claimed authority records, *id*. at 49–51, and that one skilled in the art would have been motivated to place Jones's authority records in Robb's dedicated area or special partition (i.e., the claimed secure partition) to provide greater security for this sensitive data. *Id*. at 55–58. Petitioner further asserts that Grawrock discloses the claimed master authority record, *id*. at 52–54, and one skilled in the art would have reason to include that feature because doing so would have "allowed the creation of a system where different users could gain access to different partitions based on whether they were assigned access by a system administrator." *Id.* at 59. Petitioner goes on to explain that Grawrock's master authority record feature "would have been viewed as being an important feature when implementing Robb in, for example, a corporate or other multi-user environment in which many users may be accessing the same host and memory, but where it is desirable to limit certain people to accessing certain data." *Id.* According to Petitioner, a skilled artisan would be motivated to place Grawrock's master authority record in Robb's dedicated area or special partition to better secure the data. *See id.*

Based on the current record and for purposes of this Decision, we agree with Petitioner's analysis. Specifically, Petitioner has shown that its proffered combination of Robb, Jones, and Grawrock teaches each limitation in claims 1–5. *See* Pet. 42–63. In addition, Petitioner has articulated sufficient reasoning with some rational underpinning to support the legal conclusion that its proffered combination would have been obvious to one skilled in the art. *See KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007).

Patent Owner asserts Petitioner's obviousness challenge fails to account for several claim elements. We address Patent Owner's arguments below.

b. "firmware for reading data from and writing data to the storage medium"

Patent Owner asserts "Robb does not disclose firmware for reading data from and writing data to the storage medium." Prelim. Resp. 42. We disagree. As Petitioner notes, Robb's supervisor firmware "'controls the transfer of information to and from the storage medium via the interface to the computer system,' and can 'allow/restrict/prohibit, read/write operations upon the storage medium.'" Pet. 47–48 (quoting Ex. 1007). Robb further characterizes its supervisor firmware as "integrat[ed] . . . into the existing control firmware of the hard disk drive, ensuring that no interface request is serviced before the Supervisor firmware has checked and validated the request." Ex. 1007, 10:24–27. In light of those disclosures, we agree with Petitioner that Robb discloses firmware for reading data from and writing data to the storage medium.

Patent Owner's distinction between firmware "used to control" reading and writing operations and firmware that actually does the reading

and writing operations itself (*see* Prelim. Resp. 42–43) does not distinguish over the claim limitation at issue. Because Robb's firmware is active in the individual read and write operations—including controlling these operations, acting as "traffic cop," allowing, restricting, and prohibiting the operations, *id.*—it is firmware for reading data from and writing data to the storage medium.

c. "the secure data partition for storing . . . one or more authority records" and "

Claim 1 requires a "secure data partition for storing . . . one or more authority records." Patent Owner asserts that Petitioner's challenge fails because in Jones, neither the password stored in CIS nor the passwords, key values, and access codes stored (i.e., the claimed authority records) are stored in a secure data partition. Prelim. Resp. 44–50. We disagree with Patent Owner's argument because it attacks the references individually rather than in combination, as Petitioner asserts. *See* Pet. 51. Patent Owner does not dispute that Jones discloses authority records. *See* Prelim. Resp. 47. As Petitioner explains, one skilled in the art would have been motivated to place Jones's authority records in Robb's secure partition to provide greater security for this sensitive data. Pet. 55–58. Thus, it does not matter whether Jones teaches storing data in a secure data partition because Petitioner relies on Robb, not Jones, for teaching that feature. *See id.*

d. "the secure data partition contains a master authority record"

Claim 1 recites "the secure data partition contains a master authority record." Patent Owner asserts that Petitioner's challenge fails because Grawrock's administrator record (i.e., the claimed master authority record) is not stored in a secure data partition. Prelim. Resp. 51. We disagree. This argument again attacks the references individually rather than in

combination, as Petitioner asserts. *See* Pet. 53–54, 58–59. As Petitioner explains, a skilled artisan would be motivated to place Grawrock's master authority record in Robb's secure partition to better secure the data. *See id.* at 59. Thus, it does not matter whether Grawrock teaches storing its master authority record in a secure data partition because Petitioner relies on Robb, not Grawrock, for teaching that feature. *See id*.

III. CONCLUSION

For the foregoing reasons, we determine that the information presented in the Petition establishes a reasonable likelihood that Petitioner would prevail in showing claims 1–5 unpatentable. We therefore institute an *inter partes* review of claims 1–5.

IV. ORDER

Accordingly, it is:

ORDERED that pursuant to 35 U.S.C. § 314(a), an *inter partes* review of claims 1–5 of the '020 patent is hereby instituted on the grounds presented in the Petition;

FURTHER ORDERED that no other grounds are authorized for *inter partes* review; and

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial.

PETITIONER:

Andrew R. Sommer
Ming Hung Hung
WINSTON & STRAWN LLP
asommer@winston.com
mhung@winston.com

Jonathan R. Bowser
Jonathan Stroud
UNIFIED PATENTS INC.
jbowser@unifiedpatents.com
jonathan@unifiedpatents.com

PATENT OWNER:

Cabrach Connor
Enrique Sanchez, Jr.,
CONNOR KUDLAC LEE PLLC
cab@connorkudlaclee.com
rsanchez@whitakerchalk.com