

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION**

TRUE SIGHT COMMUNICATIONS LLC,	§	Case No. 2:24-cv-00186-JRG
	§	
Plaintiff,	§	<u>JURY TRIAL DEMANDED</u>
	§	
v.	§	
	§	
TRANSCEND INFORMATION INC.,	§	
	§	
Defendant.	§	

**PLAINTIFF’S DISCLOSURE OF ASSERTED CLAIMS
AND INFRINGEMENT CONTENTIONS**

Plaintiff Truesight Communications LLC (“Truesight” or “Plaintiff”) hereby makes the following infringement disclosures under the Patent Local Rules with respect to U.S. Patent No. 8,977,783 (the “’783 Patent”) (the “Asserted Patent”). Truesight’s investigation is ongoing and discovery is not open. Accordingly, these disclosures are based on information available to Truesight at this time. Truesight reserves the right to supplement these disclosures after further discovery from defendant and non-parties, particularly documents and other discovery regarding Defendant’s accused devices. Truesight also reserves the right to assert additional claims of the Asserted Patent, accuse different products, or find alternative literal and/or equivalent infringing elements in Defendant’s products.

I. DISCLOSURE OF ASSERTED CLAIMS AND INFRINGEMENT CONTENTIONS PURSUANT TO PATENT LOCAL RULE 3-1

A. ASSERTED CLAIMS

Defendant Transcend Information Inc. (“Transcend” or “Defendant”) has infringed and/or continues to infringe one or more of the following claims of the Asserted Patent in connection with the Accused Products set forth below:

- Claims 1 through 18 of the ’783 Patent.

B. ACCUSED INSTRUMENTALITIES

1. Accused Products

Truesight is currently aware that all versions and variants of Transcend Secure Digital (SD) cards, microSD cards, CompactFlash Cards, CFexpress cards, CFast 2.0 cards and Expansion Cards, in all configurations, made, sold, offered for sale, used, or imported in the United States since 2018 (“Accused Products”) infringe the Asserted Patent. Truesight is currently aware that certain of Defendant’s products infringe the Asserted Patent. Upon information and belief, Transcend Secure Digital (SD) cards, microSD cards, CompactFlash Cards, CFexpress cards, CFast 2.0 cards, Expansion Cards, External SSDs, and Internal SSDs (such as PCIe M.2 SSDs, SATA III M.2 SSDs, 2.5” SSDs, and mSATA SSDs), in all configurations, include technology which infringe the Asserted Patent. For example, and without limitation, exemplar infringing Transcend products, include at least the following: Transcend SD cards SDC700S, Transcend SD cards SDC500S, Transcend SD cards SDC340S, Transcend SD cards SDC300S, Transcend micro SD cards USD500S, Transcend micro SD card USD340S, Transcend micro SD cards USD300S, Transcend micro SD cards USD350V, Transcend micro SD cards USDC10V, Transcend CFexpress cards CFexpress 860, Transcend CFexpress cards CFexpress 820, Transcend CompactFlash 1000 Cards, Transcend CompactFlash 800 Cards, Transcend CompactFlash 133

Cards, Transcend CFast 2.0 CFX650 cards, Transcend Expansion cards for Mac JetDrive Lite 330, Transcend Expansion cards for Mac JetDrive Lite 130, Transcend Expansion cards for Mac JetDrive Lite 350, and Transcend Expansion cards for Mac JetDrive Lite 360, alone or in combination with certain applications and software, among other products; and other infringing technology Transcend sold, imported, or used in the United States since 2018, and Transcend Secure Digital (SD) card, microSD cards, CompactFlash Cards, CFexpress cards, CFast 2.0 cards and Expansion Cards sold, imported, or used in the United States since 2018 by Transcend customers.¹

2. Claim Charts

A claim chart identifying a location of every element of every asserted claim of the '783 Patent within the Accused Products is attached hereto as **Appendix A**. Truesight believes that the Accused Products cited in the claim charts are representative of the Accused Products, including all generations and versions.

Truesight reserves the right to amend these claim charts, as well as other information contained in this document and the Appendix attached hereto, to incorporate new information learned during the course of discovery including, but not limited to, information that is not publicly available or readily discernible without discovery. Truesight further reserves the right to amend these claim charts, as well as other information contained in this document and the exhibits attached hereto, pursuant to Patent Local Rules 3-1 and 3-6, and the Court's Standing Proposed Discovery Order Section 3(a)(i).

C. LITERAL INFRINGEMENT AND DOCTRINE OF EQUIVALENTS

¹ Truesight has provided additional information regarding certain aspects of the Accused Products in the attached claim charts of **Appendix A**.

Truesight asserts that, under the proper construction of the asserted claims and their claim terms, the limitations of the asserted claims of the Truesight patent are literally present in the Accused Products, as set forth in the claim chart attached hereto as **Appendix A**. Truesight contends that any and all elements found not to be literally infringed are infringed under the doctrine of equivalents because the differences between the claimed inventions and the accused instrumentalities, if any, are insubstantial.

Truesight also contends that Defendant has directly infringed and/or continues to directly infringe the asserted claims by making, using offering for sale, selling, and importing into the United States the accused instrumentalities. Moreover, Defendant has directly infringed and/or continues to directly infringe the asserted method claims by using (*i.e.*, Defendant's employees testing and/or servicing the accused instrumentalities) in the United States. Furthermore, Defendant has indirectly infringed and/or continues to indirectly infringe by contributing to and/or inducing others (*e.g.*, Defendant's suppliers, Defendant's customers or its customers' customers) to directly infringe those claims by making, using, offering for sale, or selling the Accused Products. Such indirect infringement is further evidenced by Defendant's technical materials and marketing materials including, but not limited to, marketing materials, product briefs, product specifications, troubleshooting guides, technical support websites, reference manuals, and other business documents and communications conveyed to Defendant's customers.

Truesight also contends that Defendant has contributorily infringed and/or continues to contributorily infringe with the knowledge that the Accused Products, or the use thereof, infringe the Asserted Patent. Defendant has knowingly and intentionally contributed to the direct infringement of the Asserted Patent by others, by supplying the Accused Products and/or associated software, that embody a material part of the claimed invention of the Asserted Patent,

that are known by Defendant to be specially made or adapted for use in an infringing manner, and are not staple articles with substantial non-infringing uses.

Pursuant to Patent Local Rule 3-6(a)(1), Truesight reserves the right to amend its infringement contentions as to literal infringement or infringement under the doctrine of equivalents in light of the Court's claim construction.

D. APPLICATION PRIORITY DATES

Each of the asserted claims of the '783 Patent claim priority to U.S. Provisional Patent Application No. 61/253,789, filed on October 21, 2009.

E. PRODUCTS THAT PRACTICE THE ASSERTED PATENT

Truesight is continuing to investigate what products and/or historical products may practice the claimed inventions, including those products of third parties (*e.g.*, previous assignees) of the Asserted Patent. At the present time Truesight is not currently aware of any past products that practice its patent. Truesight's investigation is ongoing, and Truesight will supplement these contentions following its investigation (and claim construction as necessary).

II. PRODUCTION OF DOCUMENTS PURSUANT TO PATENT LOCAL RULE 3-2

Truesight is producing or making available for inspection documents that are in Truesight's possession, custody, or control as set forth in Patent Local Rule 3-2. A Truesight 3-2 Production Index identifying these documents is attached hereto.

This preliminary identification of documents is for convenience and is not an admission that each document falls within any exemplary categories in the Patent Local Rules, or that any document qualifies as prior art. Thus, Truesight reserves its right to add to, delete from, or otherwise modify its disclosures in this section as its investigation proceeds.

Production of these documents is governed by Patent Local Rule 2-2 and, with the exception of documents produced pursuant to P.R. 3.2(c) and public documents listed in the infringement charts, are considered “Confidential – Outside Attorneys Eyes Only” and disclosure of the confidential document or information, shall be limited to each parties’ outside attorney(s) of record and the employees of such outside attorney(s).

Dated: July 26, 2024

Respectfully submitted,

/s/ Vincent J. Rubino, III

Alfred R. Fabricant

NY Bar No. 2219392

Email: ffabricant@fabricantllp.com

Peter Lambrianakos

NY Bar No. 2894392

Email: plambrianakos@fabricantllp.com

Vincent J. Rubino, III

NY Bar No. 4557435

Email: vrubino@fabricantllp.com

FABRICANT LLP

411 Theodore Fremd Avenue

Suite 206 South

Rye, New York 10580

Telephone: (212) 257-5797

Facsimile: (212) 257-5796

John Andrew Rubino

NY Bar No. 5020797

Email: jarubino@rubinoip.com

Michael Mondelli III

NY Bar No. 5805114

Email: mmondelli@rubinoip.com

RUBINO IP

51 J.F.K. Parkway

Short Hills, NJ 07078

Telephone: (201) 341-9445

Facsimile: (973) 535-0921

Samuel F. Baxter

State Bar No. 01938000

Email: sbaxter@mckoolsmith.com

Jennifer L. Truelove

State Bar No. 24012906

Email: jtruelove@mckoolsmith.com

MCKOOL SMITH, P.C.

104 E. Houston Street, Suite 300

Marshall, Texas 75670

Telephone: (903) 923-9000

Facsimile: (903) 923-9099

***ATTORNEYS FOR PLAINTIFF,
TRUESIGHT COMMUNICATIONS LLC***

CERTIFICATE OF SERVICE

I hereby certify that on July 26, 2024, a true and correct copy of the above and foregoing document has been served by email on:

Christopher Kao
PILLSBURY WINTHROP SHAW PITTMAN LLP
4 Embarcadero Center, 22nd Floor
San Francisco, California 94111
Telephone: (415) 983-1000
Facsimile: (415) 983-1200

christopher.kao@pillsbury.com
Attorneys for Defendant Transcend Information Inc.

/s/ Vincent J. Rubino, III

Vincent J. Rubino, III

TRUESIGHT 3-2 PRODUCTION INDEX

3-2(c)

Bates Start	Bates End
TRUESIGHT-TRANSCEND00000001	TRUESIGHT-TRANSCEND00001080

Appendix A: Claim Chart for U.S. Patent 8,977,783

Based on information presently available, Truesight Communications LLC (“Truesight”) contends that Transcend Information Inc. (“Transcend”) infringe claims 1-18 (the “Asserted Claims”) of U.S. Patent 8,977,783 (the “’783 Patent”) through the Accused Products which are manufactured, sold, offered for sale, and/or used by Transcend.

For example, the Accused Products include, but are not limited to, all Transcend Secure Digital (SD) cards, microSD cards, CompactFlash Cards, CFexpress cards, CFast 2.0 cards, Expansion Cards, External SSDs, and Internal SSDs (such as PCIe M.2 SSDs, SATA III M.2 SSDs, 2.5” SSDs, and mSATA SSDs), in all configurations, which include, but are not limited to, the following: Transcend SD cards SDC700S, Transcend SD cards SDC500S, Transcend SD cards SDC340S, Transcend SD cards SDC300S, Transcend micro SD cards USD500S, Transcend micro SD card USD340S, Transcend micro SD cards USD300S, Transcend micro SD cards USD350V, Transcend micro SD cards USDC10V, Transcend CFexpress cards CFexpress 860, Transcend CFexpress cards CFexpress 820, Transcend CompactFlash 1000 Cards, Transcend CompactFlash 800 Cards, Transcend CompactFlash 133 Cards, Transcend CFast 2.0 CFX650 cards, Transcend Expansion cards for Mac JetDrive Lite 330, Transcend Expansion cards for Mac JetDrive Lite 130, Transcend Expansion cards for Mac JetDrive Lite 350, and Transcend Expansion cards for Mac JetDrive Lite 360, alone or in combination with certain applications and software, among other products; and other infringing technology Transcend sold, imported, or used in the United States since 2018, and Transcend Secure Digital (SD) card, microSD cards, CompactFlash Cards, CFexpress cards, CFast 2.0 cards and Expansion Cards sold, imported, or used in the United States since 2018 by Transcend customers (collectively, “Transcend Accused Products” or “Accused Products”).

Transcend directly infringes each of the Asserted Claims by importing, using, selling, and/or offering to sell the Accused Products in violation of 35 U.S.C. § 271(a).

Transcend indirectly infringes the Asserted Claims in violation of 35 U.S.C. § 271(b) by inducing third parties, including Transcend customers and end-users, to directly infringe through their operation and use of the Accused Products. Transcend has knowingly and intentionally induced this direct infringement by, *inter alia*, (i) selling, importing, or otherwise providing the Accused Products to third parties with the intent that the Accused Products will operate and be used in a manner that practices the Asserted Claims; and (ii) marketing and advertising the Accused Products. Transcend’s marketing and promotional materials for the Accused Products are found, for example, on Transcend’s website. For example, Transcend’s website offers customers downloadable User Manuals and customer support for the Accused Products that instruct customers to, among other things, set up and use the Accused Products. On information and belief, Transcend knows that its actions will result in infringement of the Asserted Claims, or subjectively believes that there is a high probability that its actions will result in infringement of the Asserted Claims but has taken deliberate actions to avoid learning these facts.

Appendix A: Claim Chart for U.S. Patent 8,977,783

Transcend also contributorily infringed each of the Asserted Claims in violation of 35 U.S.C. § 271(c) by selling, importing, and offering for sale the Accused Products, which were used to directly infringe the Asserted Claims. The Accused Products constitute a material part of the Asserted Claims.

The contentions below list certain features of the Transcend microSDHC Class 10 card that Truesight contends is representative of features of all Accused Products. The Transcend microSDHC Class 10 card is representative of all Accused Products which include, but are not limited to, Transcend SD cards and microSD cards, alone or in combination with certain streaming applications.

Truesight does not concede that any claims of the '783 Patent that are not listed below are not infringed by the identified Accused Products. Moreover, the citations to certain documents and other information below are intended to be exemplary only and in no way foreclose Truesight from citing or relying on additional documents, source code, information, and/or testimony at a later time. These contentions are preliminary in nature, and an analysis of the Accused Products, internal documentation, source code, and/or testimony from relevant witnesses may be necessary to more fully and accurately describe the infringing features of the Accused Products. Accordingly, Truesight reserves the right to supplement, correct, modify, and/or amend these contentions once such additional information is made available to Truesight. Furthermore, Truesight reserves the right to supplement, correct, modify, and/or amend these contentions as discovery in this case progresses; in view of the Court's claim construction order(s); in view of any positions taken by Transcend including, but not limited to, positions on claim construction, invalidity, and/or non-infringement; and in connection with the preparation and exchange of expert reports.

The contents of every below claim cell on which another claim cell depends are expressly incorporated by reference in that dependent cell, as if set forth in their entirety therein.

To the extent these contentions include references to entities or persons outside the Accused Products, or to the extent Transcend contends that any element of the Accused Products is attributable to a third party, Truesight contends that they are attributable to Transcend such that they constitute direct infringement by Transcend under 271(a). The acts may be attributable to Transcend because Transcend either directs or controls the others' performance, or Transcend and the other entity form a joint enterprise. *Akamai Techs., Inc. v. Limelight Networks, Inc.*, 797 F.3d 1020, 1022 (Fed. Cir. 2015). Additionally, Transcend may be vicariously liable for the activities of these other entities. *Centillion Data Sys., LLC v. Qwest Commc'ns Int'l, Inc.*, 631 F.3d 1279, 1286 (Fed. Cir. 2011). Further, the activities of these entities (including consumers or end-users), may be attributable to Transcend because Transcend (1) conditions participation in an activity or receipt of a benefit upon others' performance of one or more steps of a patented method, and (2) establishes the manner or timing of that performance. *Eli Lilly & Co. v. Teva Parenteral Medicines, Inc.*, 845 F.3d 1357, 1365 (Fed. Cir. 2017). These acts also may be attributed to Transcend because it initiated the activities of its end-users. *SiRF Tech., Inc. v. Int'l*

Appendix A: Claim Chart for U.S. Patent 8,977,783

Trade Comm’n, 601 F.3d 1319, 1330 (Fed. Cir. 2297). Further, Truesight contends that Transcend is also liable under 271(b) for inducing the acts of third parties.

Appendix A: Claim Chart for U.S. Patent 8,977,783

CLAIM	SUPPORT
1[Pre]. A kiosk for transferring content to a secure digital (SD) card, the kiosk comprising:	The Transcend Accused Products infringe directly and/or indirectly by providing a system comprising: a kiosk for transferring content to a secure digital (SD) card. This is a non-limiting preamble. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim. For example, as shown below, Transcend manufactures memory cards such as SD cards, microSD cards etc. with different memory categories for the allowing the transferring of media files. The Transcend Accused Products, including microSDHC Class 10 cards are compatible with a kiosk (<i>e.g.</i>, DV recorders, mobile phones, personal computers, etc.). The kiosks can use the SD cards by inserting it into the SD card slots. Transcend Secure Digital High Capacity (SDHC) micro cards are designed for its usage in mobile phones, personal computers and other small devices by storing the media files, documents or applications etc. The storage is done either by inserting the card in the SD cards slot of the mobile phones or by externally connecting the SD card in the personal computer USB slots or adapter slot. After the connection of the SD card to the kiosks, the selected content or media file can be transferred to the SD card and can be stored to multiple locations or files created into the SD card.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	USDC10M The ideal choice for small form factor devices with high performance demands, Transcend's High Capacity microSD cards are specifically designed for use in digital cameras, DV recorders, mobile phones, and other small devices. To ensure reliability and endurance, these microSD cards are manufactured using brand-name MLC NAND Flash chips and undergo extensive reliability testing at all stages of production. Source: https://www.transcend-info.com/Embedded/Products/No-585
--	--

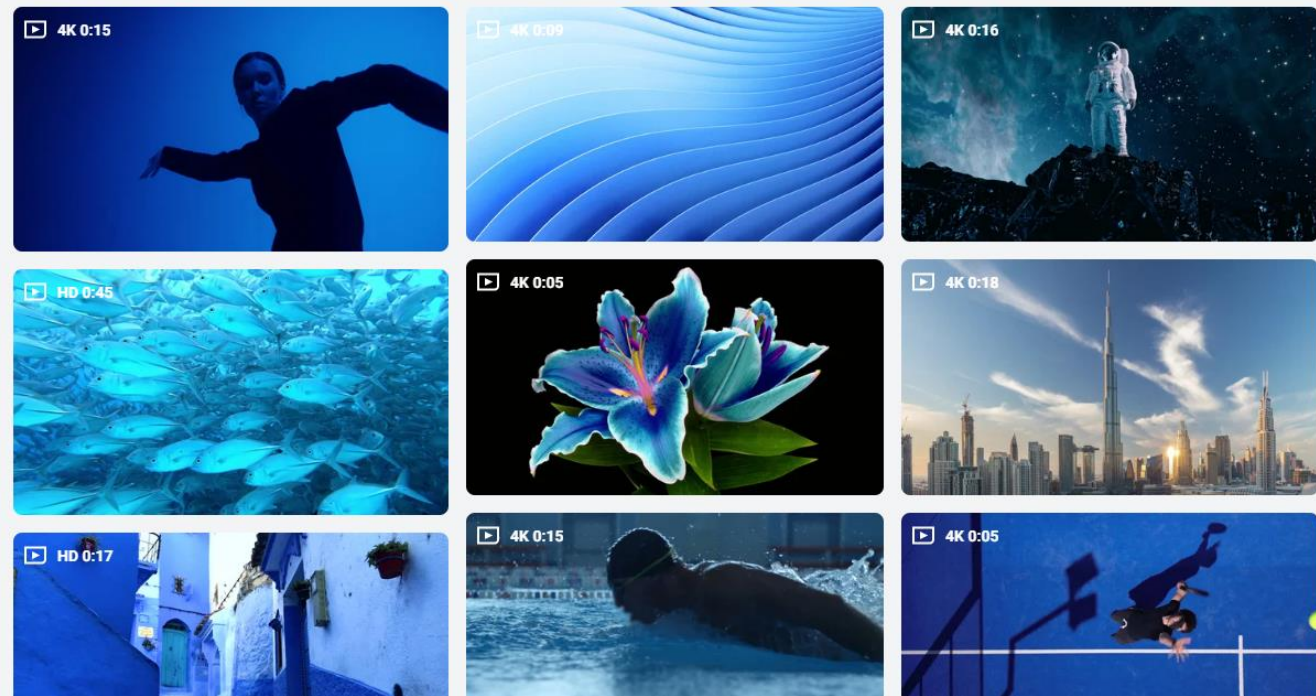
Appendix A: Claim Chart for U.S. Patent 8,977,783

	Back up files from your current PC to an external storage device 1. Connect your external storage device to your current Windows 11 PC. 2. On the taskbar, select File Explorer . 3. Locate the files you wish to copy, or the folders where those files are stored. 4. To copy multiple files, hold CTRL as you select additional files or folders. 5. Once you have files and folders highlighted, select and hold (or right-click) the folders, then select Show more options > Send to. Select your external storage device name from the list of options. 6. Your files and folders will begin copying to your drive. You may need to repeat steps 3 – 5 if you have files stored in multiple locations. Make sure to also move files from locations like your Documents, Desktop, Downloads, Favorites, Music, Podcasts, Pictures, and Videos folders. Source: https://support.microsoft.com/en-us/windows/move-your-files-to-a-new-windows-pc-using-an-external-storage-device-dd139b2e-bc73-4431-8e6e-c96e10dffdf5
1[a]. a customer interface module for receiving a customer's selection of a plurality of media files to transfer to the SD card;	Each Accused Product comprises a customer interface module for receiving a customer's selection of a plurality of media files to transfer to the SD card. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim.

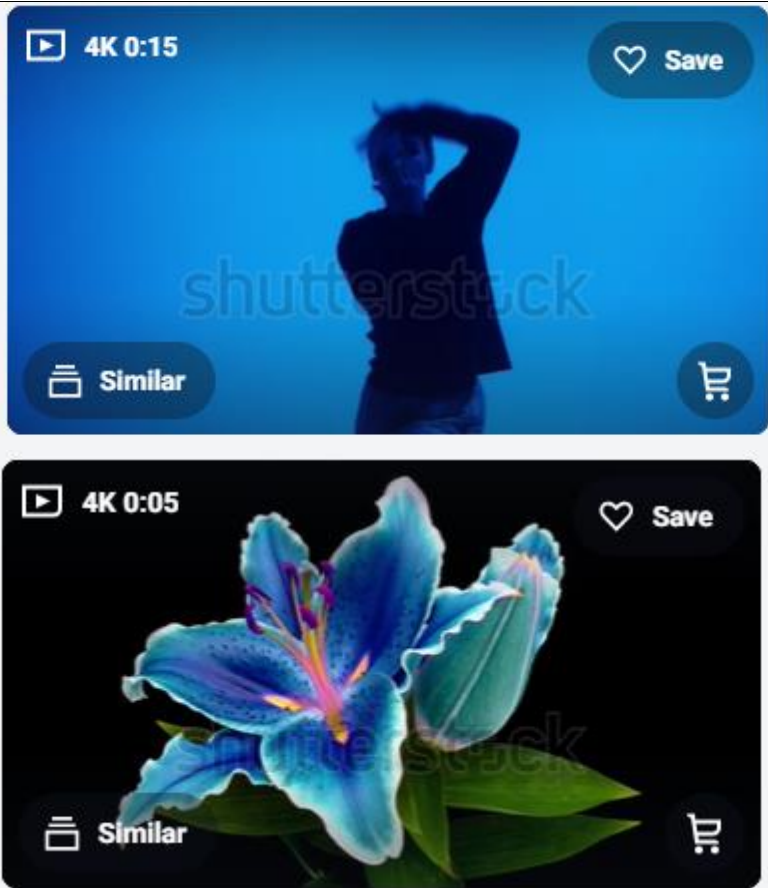
Appendix A: Claim Chart for U.S. Patent 8,977,783

For example, as shown below, when a user wants to download a group of videos to an SD card, the user accesses any website (*e.g.*, Shutterstock) containing multiple media files using the kiosk. The user can select multiple media files (*e.g.*, videos) and add those videos to the website's cart by clicking on the "Add to Cart" icon.

Following images represent series of media files that can be downloaded from 'Shutterstock' website on the kiosk.



Appendix A: Claim Chart for U.S. Patent 8,977,783

	
--	---

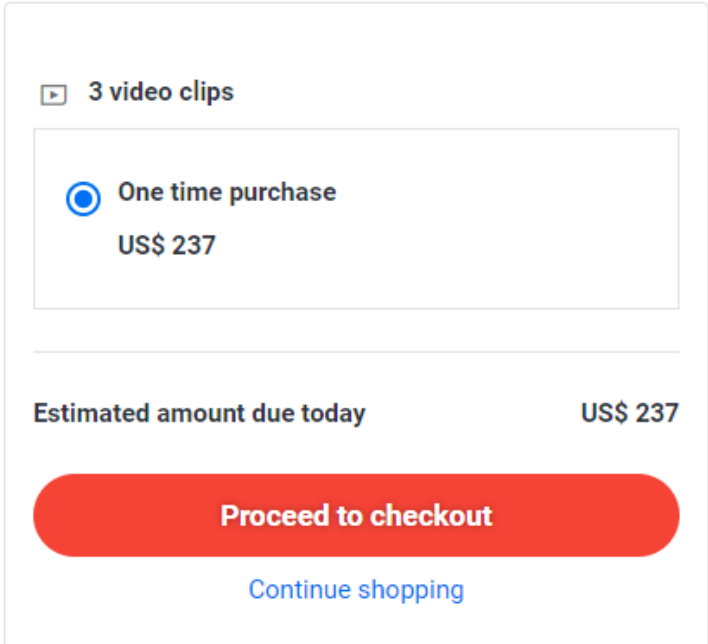
Appendix A: Claim Chart for U.S. Patent 8,977,783

	 Source: https://www.shutterstock.com/video Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
1[b]. a media file request module for requesting the plurality of media files and corresponding metadata file for each media file from a server communicatively coupled to the kiosk;	Each Accused Product comprises a media file request module for requesting the plurality of media files and corresponding metadata file for each media file from a server communicatively coupled to the kiosk. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim. For example, as shown below, a user can open the cart page on the respective website (Shutterstock) to verify the added video. Each metadata file (<i>e.g.</i>, each video has a unique video ID or file instance tied to a particular user or kiosk) associated with it, which is stored on the website's server. Further for downloading the media files, they are requested from the website's server (Shutterstock server) via the kiosk by tapping on the "Proceed to checkout" button on the "Order summary" menu.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	Your cart (3 items)  ▶ 1053787574 MOV Resolution HD US\$... ▼ Select license ⓘ ☒ Standard ☐ Enhanced Remove  ▶ 1076160860 MOV Resolution HD US\$... ▼ Select license ⓘ ☒ Standard ☐ Enhanced Remove  ▶ 1105284649 MOV Resolution HD US\$... ▼ Select license ⓘ ☒ Standard ☐ Enhanced Remove Source: https://www.shutterstock.com/video Searching for the file Since all Shutterstock content is labeled with a numerical ID, you can run a search with a particular ID to find where your image, video or music clip is on your computer.
--	--

Appendix A: Claim Chart for U.S. Patent 8,977,783

	Source: https://support.shutterstock.com/s/article/Where-are-the-files-I-downloaded?language=en_US#:~:text=Depending%20on%20your%20browser%2C%20your,from%20the%20download%20confirmation%20page. Order summary  Source: https://www.shutterstock.com/video Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
1[c]. a server interaction module for receiving the requested plurality of media files and the	Each Accused Product comprises a server interaction module for receiving the requested plurality of media files and the corresponding metadata files from the server. This element is infringed literally, or in the alternative, under the doctrine of equivalents.

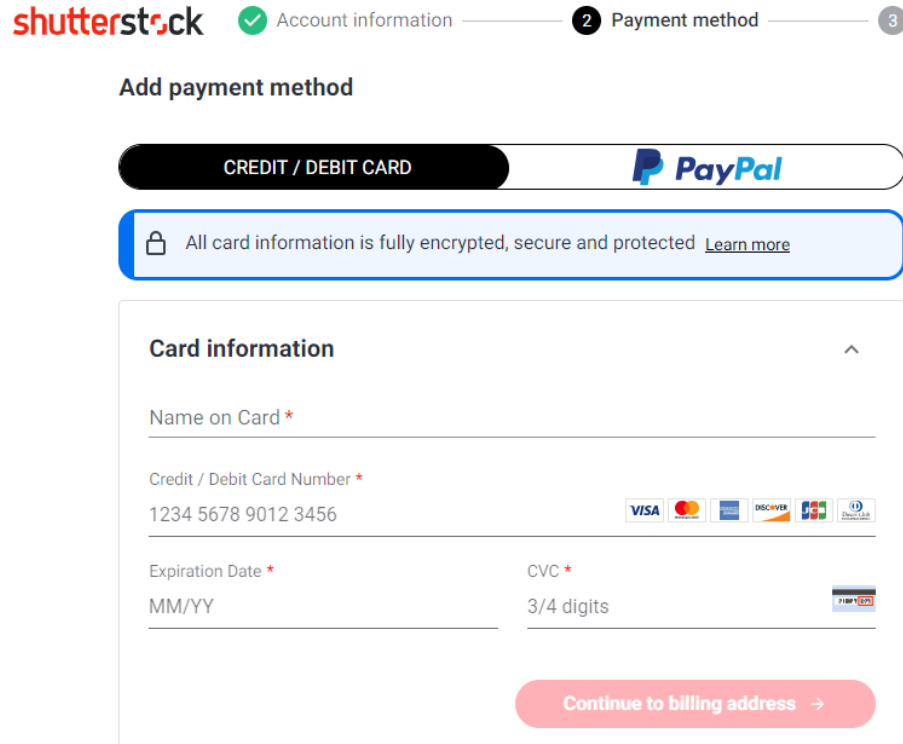
Appendix A: Claim Chart for U.S. Patent 8,977,783

corresponding metadata files from the server;	Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim. For example, as shown below, the user taps on the “Proceed to Checkout” button and downloads the videos added in the cart. The server interaction module (<i>e.g.</i>, a receiver tied to the kiosk) receives the requested plurality of media files (<i>e.g.</i>, 3 videos) along with metadata (<i>e.g.</i>, the numerical ID or file instance tied to a particular user) from the server. Order summary ▶ 3 video clips ☒ One time purchase US\$ 237 Estimated amount due today US\$ 237 Proceed to checkout Continue shopping Source: https://www.shutterstock.com/video
--	--

Appendix A: Claim Chart for U.S. Patent 8,977,783

	Searching for the file Since all Shutterstock content is labeled with a numerical ID, you can run a search with a particular ID to find where your image, video or music clip is on your computer. Source: https://support.shutterstock.com/s/article/Where-are-the-files-I-downloaded?language=en_US#:~:text=Depending%20on%20your%20browser%2C%20your,from%20the%20download%20confirmation%20page. Truesight reserves its right to identify source code under Local Rule 3-1 and the Court’s Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
1[d]. a transaction module for accepting payment from a customer for the customer's selection of the plurality of media files to transfer to the SD card;	Each Accused Product comprises a transaction module for accepting payment from a customer for the customer's selection of the plurality of media files to transfer to the SD card. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim. For example, as shown below, the transaction module (e.g., a digital wallet or digital payment processor tied to the kiosk) accepts payment from a customer for the customer’s selection of the plurality of media files to transfer to the SD card. After the payment is successful, the below website prompts the “Download location” on the kiosks for the download of the videos directly on the user’s SDHC memory card.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	A screenshot of the Shutterstock payment page. At the top, the Shutterstock logo is on the left, and a progress bar shows 'Account information' (checked), 'Payment method' (active), and a third step. Below the progress bar is the heading 'Add payment method'. There are two buttons: 'CREDIT / DEBIT CARD' (highlighted) and 'PayPal'. Below these is a blue box with a lock icon and the text 'All card information is fully encrypted, secure and protected' with a 'Learn more' link. The main form is titled 'Card information' and contains fields for 'Name on Card *', 'Credit / Debit Card Number *' (with the number 1234 5678 9012 3456 and logos for Visa, Mastercard, American Express, Discover, and others), 'Expiration Date *' (MM/YY), and 'CVC *' (3/4 digits). A pink button at the bottom right says 'Continue to billing address →'. Source: https://www.shutterstock.com/video Download location On a computer, your download will start automatically right after you license the digital asset. Depending on your browser, your file will either save directly to your browser's download folder, or you will be prompted to choose a folder in which to save the file. If your download did not start automatically, you can opt to manually start the process again from the download confirmation page. If you need to download the file again, you can always navigate to All your downloads in the Catalog and redownload the file again for free, choosing a new folder location.
--	--

Appendix A: Claim Chart for U.S. Patent 8,977,783

	Source: https://support.shutterstock.com/s/article/Where-are-the-files-I-downloaded?language=en_US#:~:text=Depending%20on%20your%20browser%2C%20your,from%20the%20download%20confirmation%20page. Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
1[e]. an SD card writer for writing data to an unsecure user area of the SD card and a protected secure area of the SD card; and	Each Accused Product comprises an SD card writer for writing data to an unsecure user area of the SD card and a protected secure area of the SD card. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim. For example, as shown below, the SD card writer (e.g., a built-in slot on the kiosk for the attachment of SDHC memory card capable of transferring data to an unsecure and secure area of the SD card) writes data to an unsecure user area and a protected secure area of the SD card. An SD memory card is an ideal way to save your PC's data, such as photos, music, emails, software, documents, and apps. You can also transfer the data to other devices, such as digital cameras or smartphones, and then store the data for future use. Once the SD card is placed in your PC's dedicated slot, you can begin saving and moving your information. Source: https://www.samsung.com/us/support/answer/ANS00061646/

Appendix A: Claim Chart for U.S. Patent 8,977,783

	The diagram illustrates the memory layout of an SD card. At the top is the 'Protected Area'. Below it is the 'User Area Partition', which contains the 'User Area' (a large orange rectangle). Below the User Area are the 'File System' and 'MBR'. Further down are 'Boot Partition 0' and 'Boot Partition 1', which are grouped by a red bracket and labeled 'New in SD 9.0'. Below the boot partitions is the 'RPMB Unit / Target', also bracketed and labeled 'New in SD 9.0'. At the bottom are the 'CSD register', 'SCR register', and 'Extension register'. On the left side, LBA addresses are marked: 'LBA=XXXXXX' for the User Area, 'LBA=000000' for the File System/MBR, 'LBA=00FFFF' for the Boot Partitions, and 'LBA=000000' for the RPMB Unit. A note at the bottom states 'LBA is indicated by sector.'. Source: https://www.sdcard.org/cms/wp-content/uploads/2022/05/Boot-TCG-and-RPMB-The-New-Security-Features-Introduced-in-SD-9.0.pdf Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
1[f]. a media file processing module for preparing the plurality of media files and the corresponding metadata files to be written to the SD card in cooperation with the SD card writer, wherein	Each Accused Product comprises a media file processing module for preparing the plurality of media files and the corresponding metadata files to be written to the SD card in cooperation with the SD card writer, wherein space is pre-allocated on the SD card for writing an encrypted playable content portion of each media file to an unsecure area of the SD card, and wherein, except for a user key, data to be written to the unsecure area of the SD card is queued for writing in advance of data to be written to a secure area of the SD card, such that the data to be written to the unsecure area is written in time before the data to be written to the secure area is written, and wherein the playable media files are encrypted by a content key that is encrypted by the user key.

Appendix A: Claim Chart for U.S. Patent 8,977,783

space is pre-allocated on the SD card for writing an encrypted playable content portion of each media file to an unsecure area of the SD card, and wherein, except for a user key, data to be written to the unsecure area of the SD card is queued for writing in advance of data to be written to a secure area of the SD card, such that the data to be written to the unsecure area is written in time before the data to be written to the secure area is written, and wherein the playable media files are encrypted by a content key that is encrypted by the user key.	This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim. <i>See supporting evidence for claims 1[d] and 1[e].</i> For example, as shown below, a media file processing module prepares media files and metadata files to be written to the SD card in secure and unsecure areas. Logical locations of CPRM components are defined for the “SD memory card”. As per the figures, a pre-allocated space on the SD card (<i>e.g.</i>, user data area) is defined for the encrypted content / files (playable content of the media file). The corresponding playable media content is encrypted using a series of keys. 3.3 CPRM Components This section describes the logical location and format of the CPRM components, when stored on the "SD Memory Card." Figure 3-1 depicts the logical locations of CPRM Components on the "SD Memory Card." These logical locations are used, unless explicitly noted otherwise in an application specific part of <i>CPRM SD Memory Card Book</i>.
---	--

Appendix A: Claim Chart for U.S. Patent 8,977,783

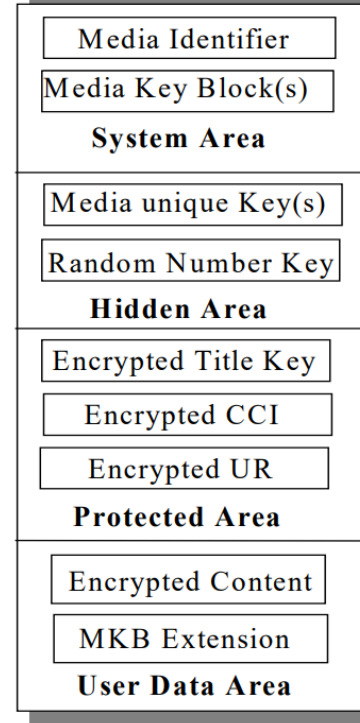


Figure 3-1 – SD Memory Card

- A Media Identifier (ID_{media}) and sixteen Media Key Blocks are pre-recorded in the System Area.
- Sixteen Media Unique Keys and Random Number Key are pre-recorded in the Hidden Area.
- Encrypted Title Keys, Encrypted CCI (Copy Control Information) and Encrypted UR (Usage Rules) are recorded in the Protected Area.
- Encrypted Content and MKB Extension are recorded in the User Data Area

Source: <http://www.4centity.com/document.aspx?doc=2ef45977-c7fd-45f5-b2bf-759ac88764d3>

Appendix A: Claim Chart for U.S. Patent 8,977,783

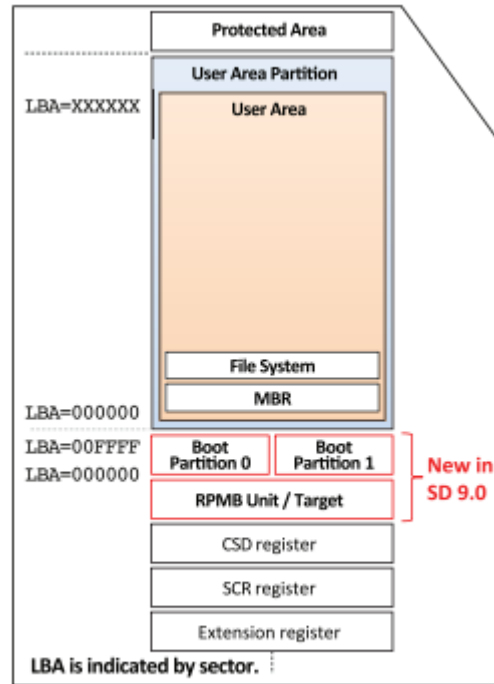


Figure 1-1
Newly added memory structure for Boot and RPMB

Source: <https://www.sdcard.org/cms/wp-content/uploads/2022/05/Boot-TCG-and-RPMB-The-New-Security-Featu-res-Introduced-in-SD-9.0.pdf>

3.6.1.1 ASF File Encryption

SD-Video application treats the Microsoft's Advanced Systems Format (ASF) file as one of the file format that contains video stream. The ASF file is encrypted by the Title Key as follows:

- The ASF file consists of an ASF Header Section, ASF Data Section Object (fixed to 50 bytes) and multiple ASF Data Packets.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	• The ASF Header Section and the ASF Data Section Object are not encrypted. • Each ASF Data Packet consists of a header part (variable size M: less than or equal to 40 bytes) and a data part (variable size N). Size of Data Packet is less than 2^{32} bytes. • Each ASF Data Packet is encrypted by the corresponding Title Key using C2_ECBC (the C2 cipher algorithm in C-CBC mode) as follows. Source: http://www.4centity.com/document.aspx?doc=d1aa7cfa-4541-4fb4-a46c-ae030413bc4 For example, as shown below, during the writing process of large media files on the SDHC memory card, a writable space is allocated, called as “directory blocks”. These blocks can be allocated at once (written together) while writing on the memory card. The directory blocks for all the media content are can be (<i>e.g.</i>, allocated) in the first stage and queued, all at once as depicted in the image below. These directory blocks can be followed by the data blocks containing the encrypted content of the media file. Multiple data blocks are pointed by each directory block and can be arranged and queued sequentially or in a regular serial number. For example, the respective directories (<i>e.g.</i>, PRG001, PRG003 etc.) can be allocated together at the same time. The media content (<i>e.g.</i>, MOV00X.SFX, MOV00X.SMX etc.) is encrypted sequentially, having a serial number for each of the data blocks. For example, after the media files are stored in the user data area in the form of data blocks, the content and the usage rules encryption and can be stored in the protected or secure area. For example, as shown below, during encryption of the content, the media unique key which is generated by the media key and the media id, is used for the encryption of Title key and Usage rules which is encrypted and further decrypted (C2_DCBC) using a session key (Ks).
--	---

Appendix A: Claim Chart for U.S. Patent 8,977,783

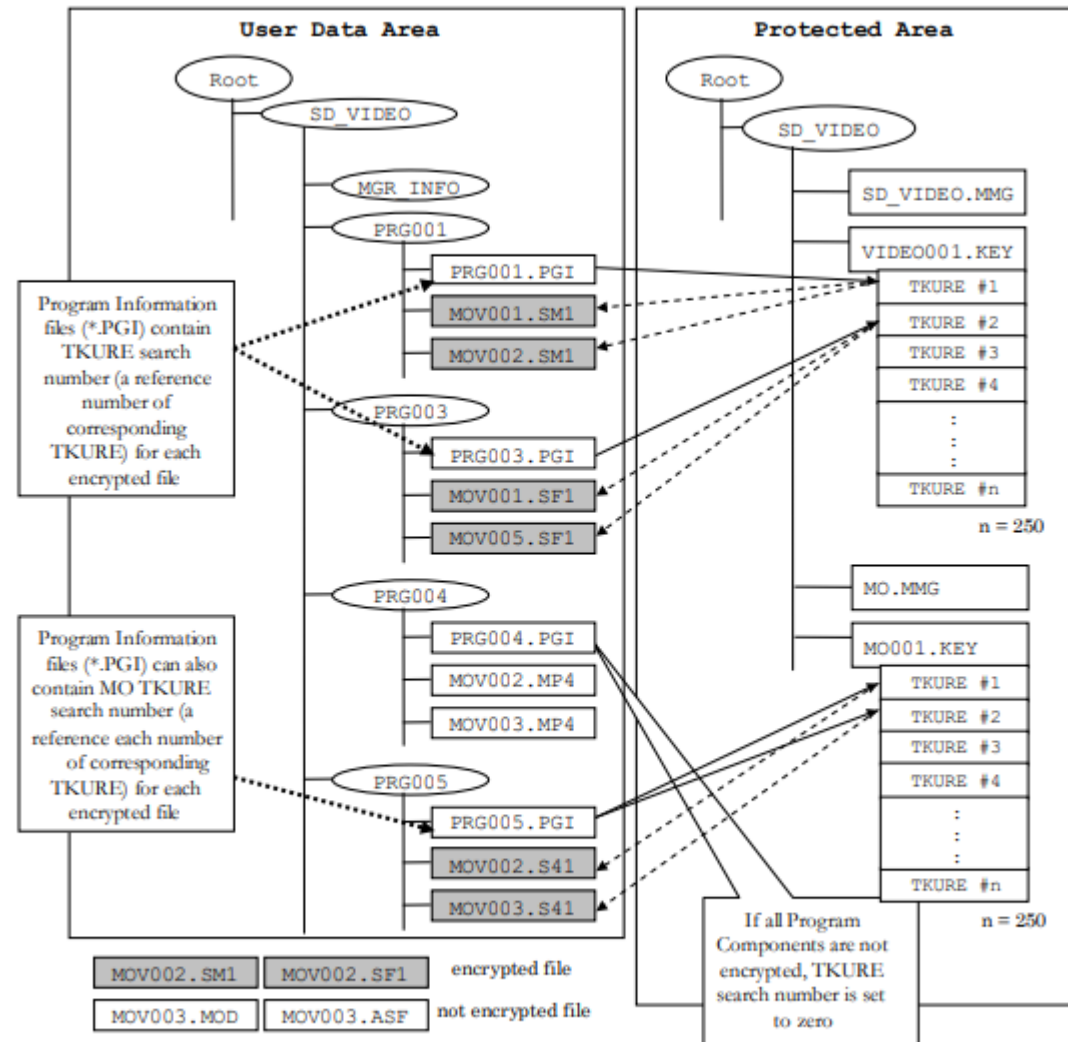


Figure 3-4 Relationship between Directory and Filename

Source: <http://www.4centity.com/document.aspx?doc=d1aa7cfa-4541-4fb4-a46c-ae030413bc4>

Appendix A: Claim Chart for U.S. Patent 8,977,783

	In an SD Memory Card, two kinds of key are stored. One is called a content key which is used to encrypt corresponding content. The other is called a User Key which is used to protect the Content Key values and its usage rules. These keys can be also delivered separately. An example of separate distribution is drawn in Figure 3-1. Source: http://www.4centity.com/document.aspx?doc=868ca775-0fcb-4350-8c19-9860830072d9 3.3.4 User Data Area The SD Memory Card shall contain a User Data Area, which is a user-accessible read/write area that is used to store Encrypted content. User Data Area may also contain other user data. When the SD Memory Card is connected to a PC, the user data area typically looks like a normal disk. 3.3.4.1 Encrypted content In the SD Memory Card, each piece of content to be protected shall be encrypted with a unique Title Key, and stored as an encrypted file in the User Data Area. The file system of the User Data Area is typically a FAT12, FAT16, FAT32 or exFAT file system. The directory structure and file names of the encrypted content are defined in each application specific part of the <i>CPRM SD Memory Card Book</i>. Source: http://www.4centity.com/document.aspx?doc=2ef45977-c7fd-45f5-b2bf-759ac88764d3
--	---

Appendix A: Claim Chart for U.S. Patent 8,977,783

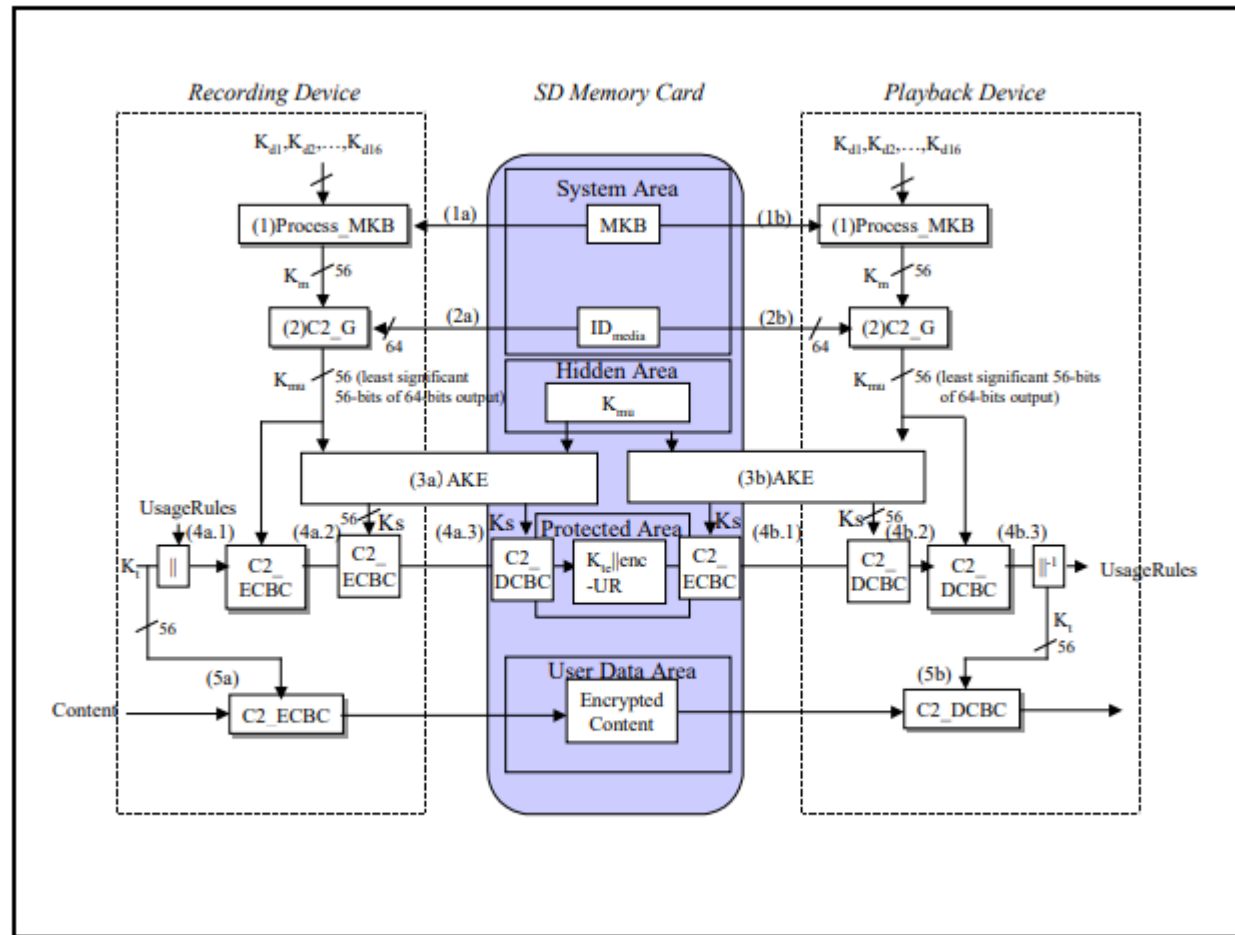


Figure 3-1 Content Encryption and Decryption on SD Memory Card

Appendix A: Claim Chart for U.S. Patent 8,977,783

	3.6.1.1 ASF File Encryption SD-Video application treats the Microsoft's Advanced Systems Format (ASF) file as one of the file format that contains video stream. The ASF file is encrypted by the Title Key as follows: • The ASF file consists of an ASF Header Section, ASF Data Section Object (fixed to 50 bytes) and multiple ASF Data Packets. • The ASF Header Section and the ASF Data Section Object are not encrypted. • Each ASF Data Packet consists of a header part (variable size M: less than or equal to 40 bytes) and a data part (variable size N). Size of Data Packet is less than 2^{32} bytes. • Each ASF Data Packet is encrypted by the corresponding Title Key using C2_ECBC (the C2 cipher algorithm in C-CBC mode) as follows. Source: http://www.4centity.com/document.aspx?doc=d1aa7cfa-4541-4fb4-a46c-ae030413bc4 -(4a) Title Key and Usage Rule Encryption process. The following steps (4a.1) through (4a.3) describe the Title Key and Usage Rule Encryption Process. When the content is encrypted, a Title Key is picked at random. (4a.1) Encrypt the Title Key and Usage Rule Entry by the Media Unique Key associated with MKB. The Recording Device encrypts the Title Key and Usage Rule Entry (see Table 3-10), as a single 64-byte encryption frame using the Media Unique Key associated with MKB. The encryption algorithm is C2_ECBC (the C2 cipher algorithm in C-CBC mode) which is described in the <i>Introduction and Common Cryptographic Elements</i> book. (4a.2) Encrypt the Title Key and Usage Rule Entry by the Session Key.
--	---

Appendix A: Claim Chart for U.S. Patent 8,977,783

The Recording Device further encrypts the entire 64-byte Title Key and Usage Rule Entry using the Session Key K_s , which is shared at step (3a), using C2_ECBC.

The results (the doubly-encrypted Title Key and Usage Rules) are sent to the SD Memory Card.

(4a.3) Decrypt the Title Key and Usage Rule Entry by the Session Key.

In the SD Memory Card, the doubly-encrypted 64-byte Title Key and Usage Rule Entry is decrypted using the Session Key K_s , which is shared at step (3a). The decryption algorithm is C2_DCBC (the C2 cipher algorithm in C-CBC mode) which is described in the *Introduction and Common Cryptographic Elements* book. The result (the encrypted Title Key and Usage Rule Entry) is stored in the Protected Area.

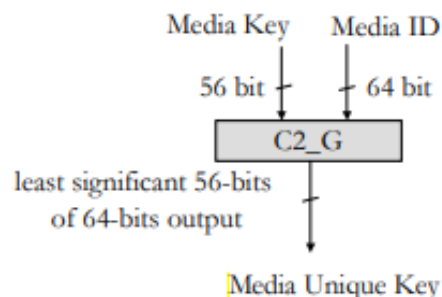
Source: <http://www.4centity.com/document.aspx?doc=d1aa7cfa-4541-4fb4-a46c-ae030413bc4>

Each encrypted content file in the User Data Area is associated with the corresponding TKURE for Programs in the Protected Area through its TKURE_SRN for Programs in case of Program Encryption.

Source: <http://www.4centity.com/document.aspx?doc=d1aa7cfa-4541-4fb4-a46c-ae030413bc4>

Note that the Recording Device does not need to write User Key, Content Key and content to an SD Memory Card at a time. For example, there is a case that a Recording Device stores only one User Key and several Content Keys into an SD Memory Card, but does not store the corresponding content data at the time.

Source: <http://www.4centity.com/document.aspx?doc=868ca775-0fcb-4350-8c19-9860830072d9>



Appendix A: Claim Chart for U.S. Patent 8,977,783

	Source: http://www.4centity.com/document.aspx?doc=2ef45977-c7fd-45f5-b2bf-759ac88764d3 Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
2. The kiosk of claim 1, further comprising a preview module for playing a preview of content of selected by the customer through the kiosk while the SD card writer writes the plurality of media files to the SD card, wherein the preview of content selected by the customer includes content from the plurality of media files being written to the SD card.	Each Accused Product comprises the kiosk of claim 1, further comprising a preview module for playing a preview of content of selected by the customer through the kiosk while the SD card writer writes the plurality of media files to the SD card, wherein the preview of content selected by the customer includes content from the plurality of media files being written to the SD card. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim. For example, as shown below, the kiosk comprises a preview module, which during the writing process of the content files on the SDHC memory card, the media files can be played on the kiosk by hovering the cursor on the respective media files on the webpage while it is being written on the SDHC memory card. The images shown below represents a series of snippets taken from a video at different time frames.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	 Source: https://www.shutterstock.com/video
--	--

Appendix A: Claim Chart for U.S. Patent 8,977,783

	Download location On a computer, your download will start automatically right after you license the digital asset. Depending on your browser, your file will either save directly to your browser's download folder, or you will be prompted to choose a folder in which to save the file. If your download did not start automatically, you can opt to manually start the process again from the download confirmation page. If you need to download the file again, you can always navigate to All your downloads in the Catalog and redownload the file again for free, choosing a new folder location. Source: https://support.shutterstock.com/s/article/Where-are-the-files-I-downloaded?language=en_US#:~:text=Depending%20on%20your%20browser%2C%20your,from%20the%20download%20confirmation%20page. Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
3. The kiosk of claim 1, further comprising a firmware update module for transferring a firmware update to the SD card.	Each Accused Product comprises the kiosk of claim 1, further comprising a firmware update module for transferring a firmware update to the SD card. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim. For example, as shown below, the kiosk comprises a firmware update module which allows firmware updates to be dragged to the root directory of the memory card. Further, in the series of snippets added below from a YouTube video, the kiosk allows transferring a firmware update to the SD card by selecting the firmware file and pasting it to the SD card folder.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	What should I do if firmware upgrade fails? Category : Software / Firmware / Applications 1. Please go to the Transcend website and download the latest firmware for your model: https://www.transcend-info.com/support/cate-228 2. On a PC, drag the .bin file from the archive to the root directory of your memory card. Make sure it is not in any folders. 3. Insert the memory card in the DrivePro and power the DrivePro on (by connecting it to power). A second firmware upgrade will start automatically. Source: https://www.transcend-info.com/Support/FAQ-1180
--	---

Appendix A: Claim Chart for U.S. Patent 8,977,783



Copying Firmware to SD Card

 **SolarEdge North America**
3.33K subscribers

Subscribe

 15



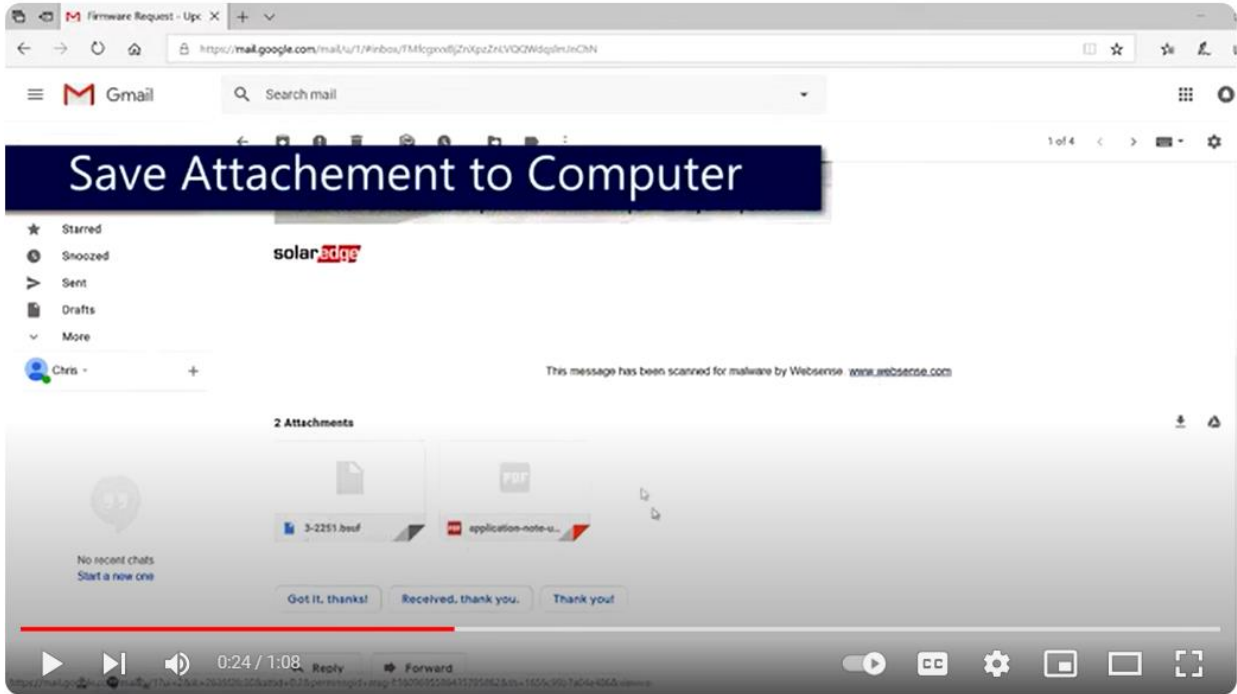
 Share

 Download



Source: https://www.youtube.com/watch?v=2Le8ND4LX_I

Appendix A: Claim Chart for U.S. Patent 8,977,783



Save Attachment to Computer

Starred
Snoozed
Sent
Drafts
More

Chris - +

This message has been scanned for malware by Websense. www.websense.com

2 Attachments

3-2251.beef application-note-u...

Got it, thanks! Received, thank you. Thank you!

0:24 / 1:08

Reply Forward

Copying Firmware to SD Card

SolarEdge North America
3.33K subscribers

Subscribe

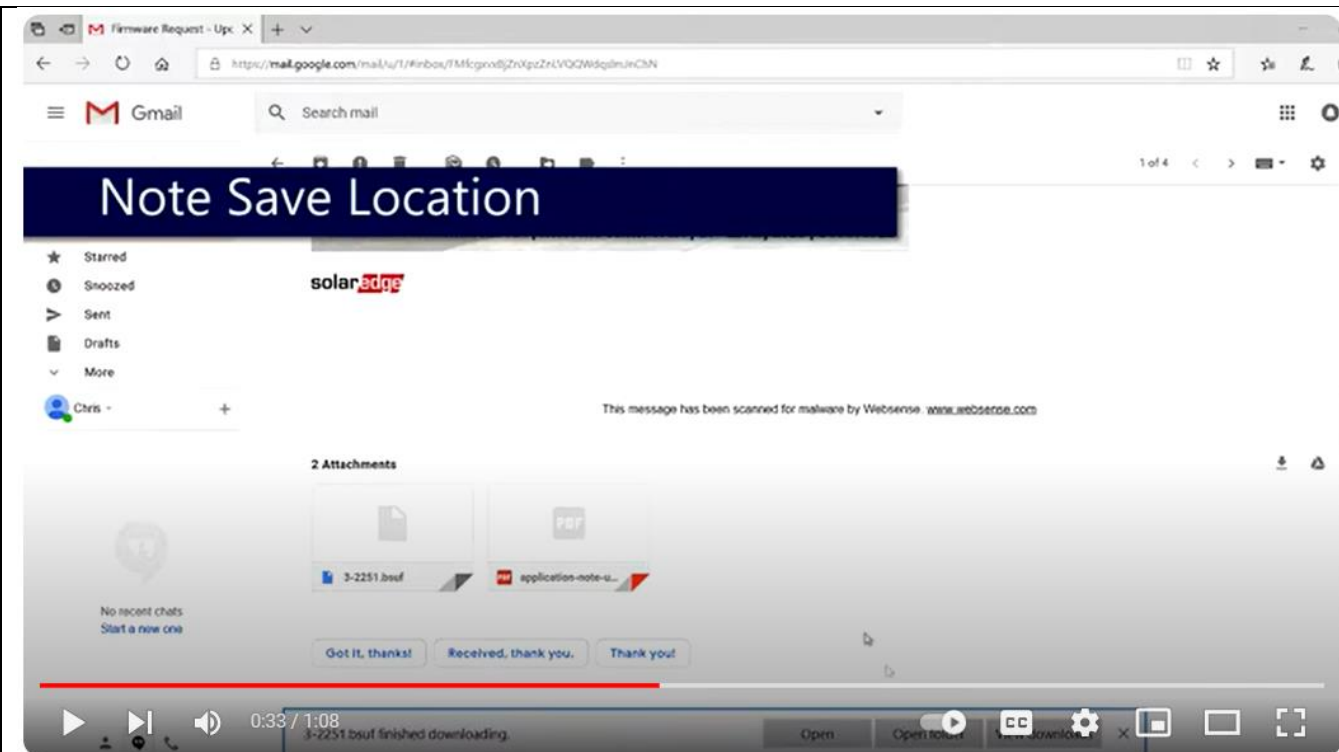
15

Share

Download

Source: https://www.youtube.com/watch?v=2Le8ND4LX_I

Appendix A: Claim Chart for U.S. Patent 8,977,783



Note Save Location

solar_{edge}

This message has been scanned for malware by Websense. www.websense.com

2 Attachments

3-2251.bsuf application-note-u...

Got it, thanks! Received, thank you. Thank you!

0:33 / 1:08

3-2251.bsuf finished downloading.

Open Open folder Download

Copying Firmware to SD Card

solar_{edge} SolarEdge North America
3.33K subscribers

Subscribe

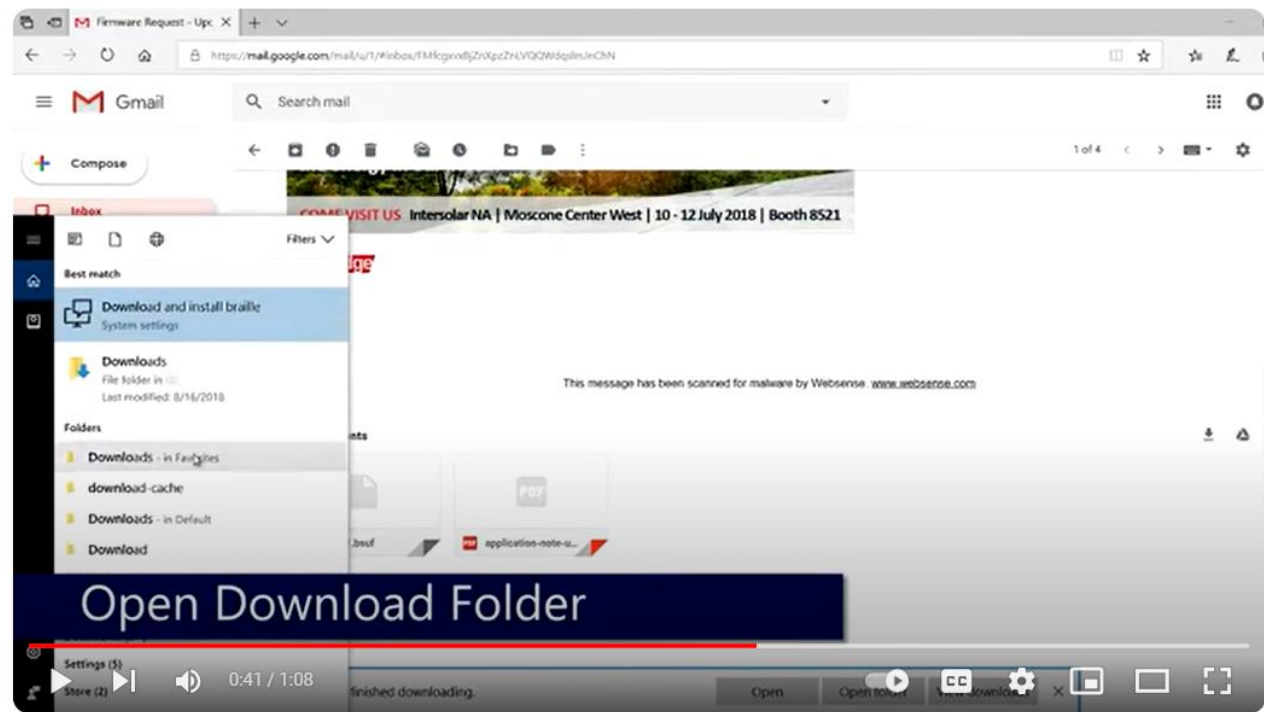
15 Likes

Share

Download

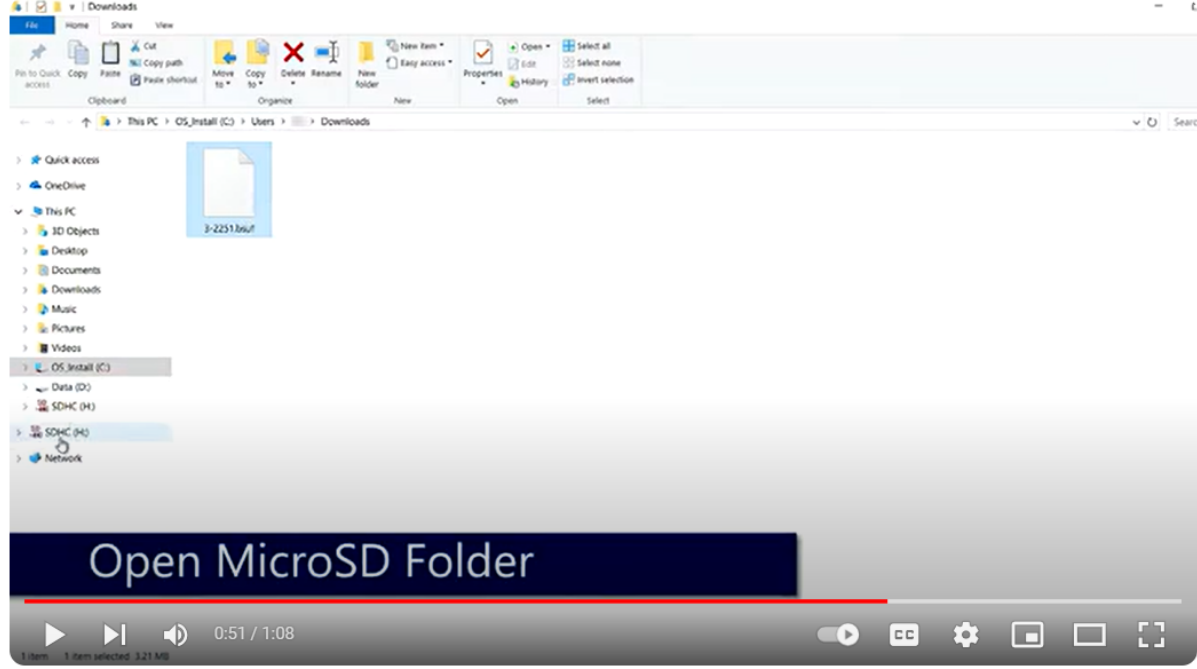
Source: https://www.youtube.com/watch?v=2Le8ND4LX_I

Appendix A: Claim Chart for U.S. Patent 8,977,783



Source: https://www.youtube.com/watch?v=2Le8ND4LX_I

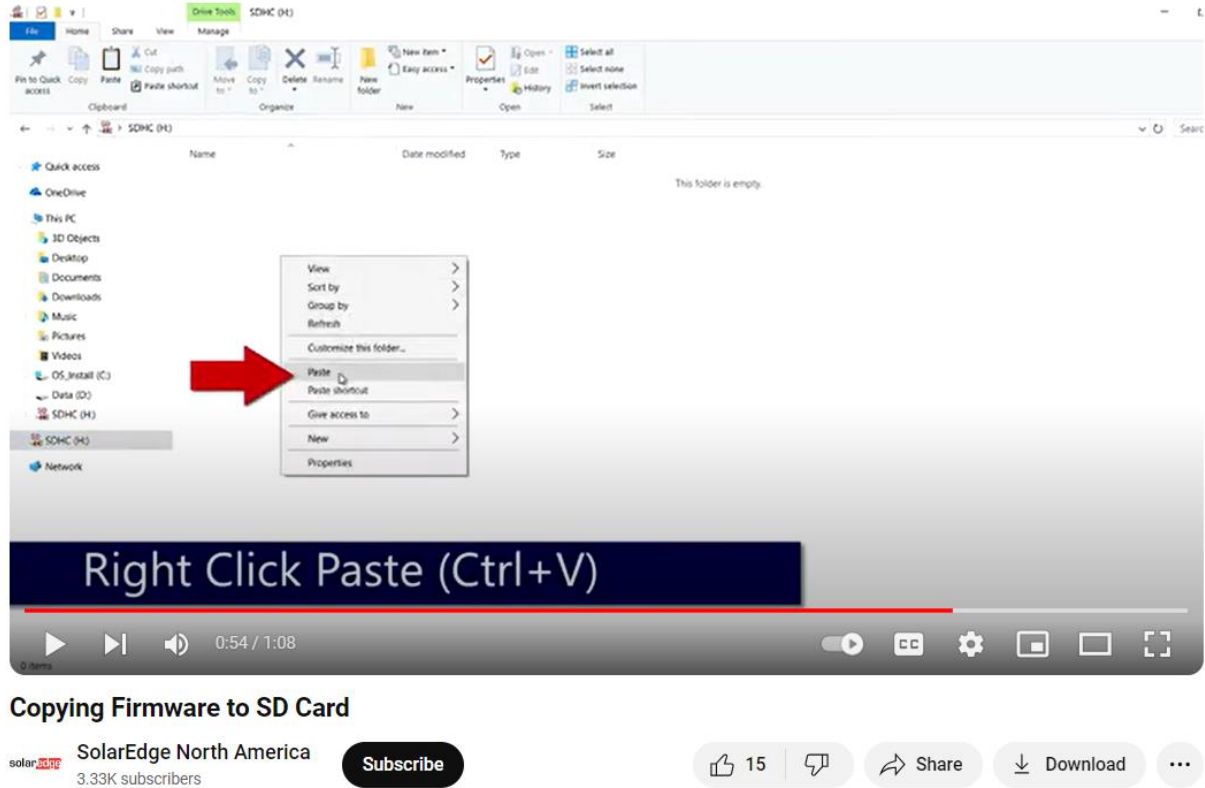
Appendix A: Claim Chart for U.S. Patent 8,977,783



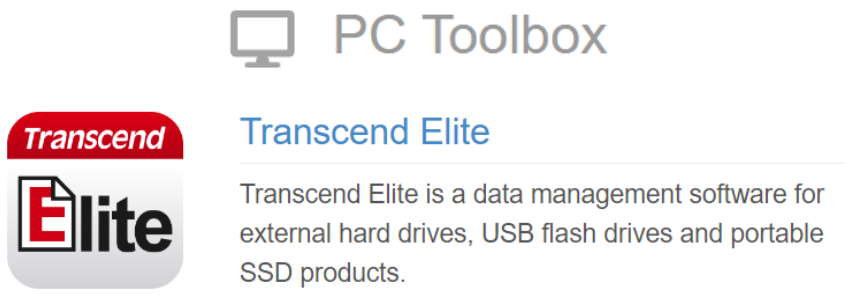
The screenshot shows a Windows file explorer window titled 'Downloads'. The address bar indicates the path: 'This PC > OS_Install (C:) > Users > Downloads'. The left sidebar shows the 'Downloads' folder selected. The main area displays a single file named '3-2231.buff'. A video player overlay is present, showing the title 'Open MicroSD Folder' and a progress bar at 0:51 / 1:08. Below the video player, the video title 'Copying Firmware to SD Card' is displayed, along with the channel name 'SolarEdge North America' and 3.33K subscribers. The video has 15 likes and a 'Subscribe' button. The video player controls include play, pause, volume, and full screen buttons.

Source: https://www.youtube.com/watch?v=2Le8ND4LX_I

Appendix A: Claim Chart for U.S. Patent 8,977,783

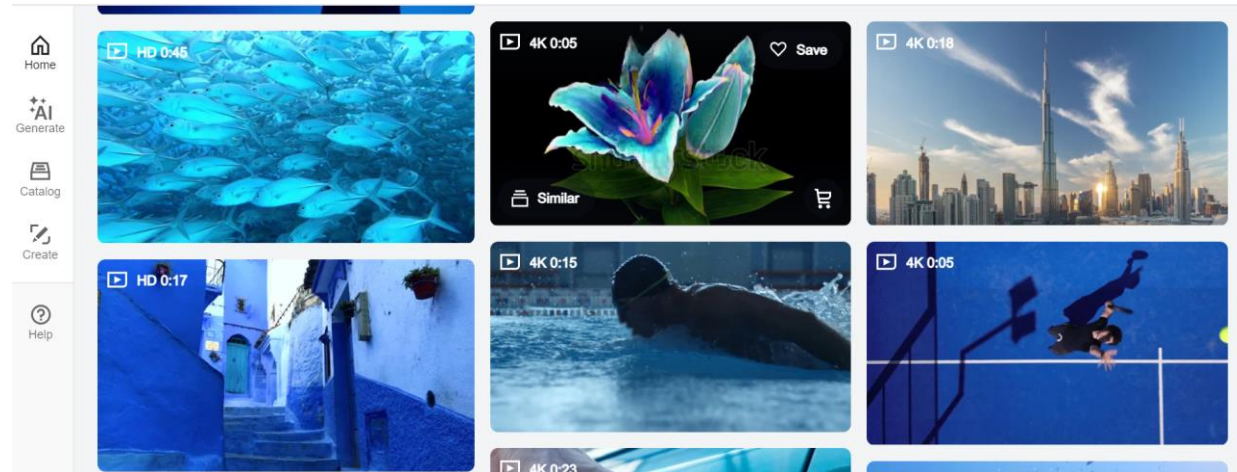
	 Right Click Paste (Ctrl+V) Copying Firmware to SD Card SolarEdge North America 3.33K subscribers Source: https://www.youtube.com/watch?v=2Le8ND4LX_I
4. The kiosk of claim 1, further comprising a software player update module for transferring a software player update to the SD card.	Each Accused Product comprises the kiosk of claim 1, further comprising a software player update module for transferring a software player update to the SD card. This element is infringed literally, or in the alternative, under the doctrine of equivalents.

Appendix A: Claim Chart for U.S. Patent 8,977,783

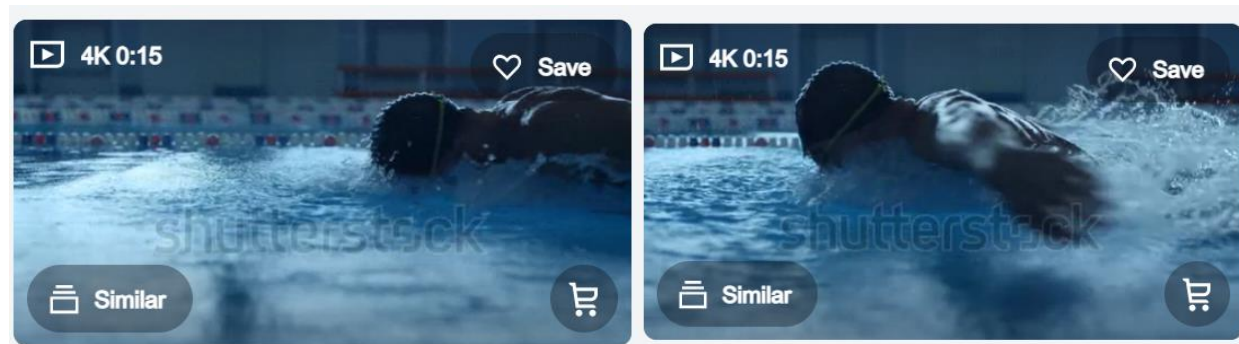
	Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim. For example, as shown below, the kiosk comprises a software player update module which allows software downloads to the kiosk. Among these software tools, Transcend Elite is a data management software for portable SSD products. The image is a screenshot of a web page titled "PC Toolbox" with a computer monitor icon. Below the title, there is a section for "Transcend Elite" featuring the Transcend logo (a red bar with "Transcend" in white) and the "Elite" logo (a stylized "E" with "lite" in black). To the right of the logos, the text reads: "Transcend Elite is a data management software for external hard drives, USB flash drives and portable SSD products." Source: https://www.transcend-info.com/support/software <i>See supporting evidence for claim 3.</i> Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
5. The kiosk of claim 1, further comprising a customer attraction module for playing segments from media files currently available for download from the kiosk while the kiosk is not used for purchase of a media file.	Each Accused Product comprises the kiosk of claim 1, further comprising a customer attraction module for playing segments from media files currently available for download from the kiosk while the kiosk is not used for purchase of a media file. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim.

Appendix A: Claim Chart for U.S. Patent 8,977,783

For example, as shown below, the kiosk comprises a customer attraction module which allows playing segments from the media files available for download when the kiosk is not getting used for purchasing any media file.



Source: <https://www.shutterstock.com/video>



Appendix A: Claim Chart for U.S. Patent 8,977,783

	Source: https://www.shutterstock.com/video Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
6. The kiosk of claim 1, further comprising a USB port to allow connection of the SD card with a USB adapter to the kiosk.	Each Accused Product comprises the kiosk of claim 1, further comprising a USB port to allow connection of the SD card with a USB adapter to the kiosk. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim. For example, as shown below, the kiosk comprises a USB port to connect any external device. The microSD cards can be inserted into an SD adapter which can be inserted into a memory card reader. Such memory card readers allow connection of SD card to the kiosk using an USB adapter.

Appendix A: Claim Chart for U.S. Patent 8,977,783

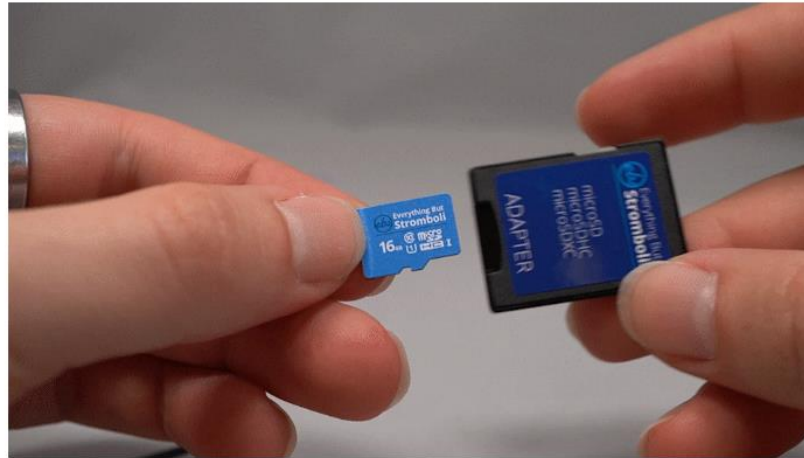
	What is a computer port? Let's start with the basics. A computer port is a "connection point or interface between a computer and an external or internal device," according to Techopedia [2]. In layman's terms, this means that you can use ports to connect different devices to your laptop or desktop, or you can use them to charge your PC. USB TYPE-A The is the most common desktop and laptop port that you'll see. This port is capable of both USB 2.0 or USB 3.0 speeds. USB Type-A is considered the original USB connector and it can connect to an almost limitless array of auxiliary devices such as external speakers, mice, and printers [10]. Source: https://www.hp.com/in-en/shop/tech-takes/post/what-desktop-computer-ports-are-available
--	--

Appendix A: Claim Chart for U.S. Patent 8,977,783

SD Card Adapters

SD Card adapters are different from readers because they do not convert across a different interface type. Adapters for SD cards only convert MicroSD or MiniSD to full sized SD.

Step 1: Put the MicroSD card into the SD Adapter



At the bottom of the adapter there is an open slot, insert your **MicroSD Card** here. Some SD Adapters also have a write-lock switch on them. Make sure this switch is unlocked or else you will only be allowed to read the data on the drive. Additionally, verify that you are using the right kind of adapter. Don't get MicroSD confused with MiniSD. MiniSD is very uncommon.

How to use an SD Adapter

EBS sells 2 kinds of adapters and readers. Regardless of what kind of adapter you have, or the manufacturer of the reader, they all work about the same.

USB-A Readers

The first are readers that convert many or one kind of memory card to a USB-A port. Your reader may operate this way if you are trying to get your photos or media onto your computer.

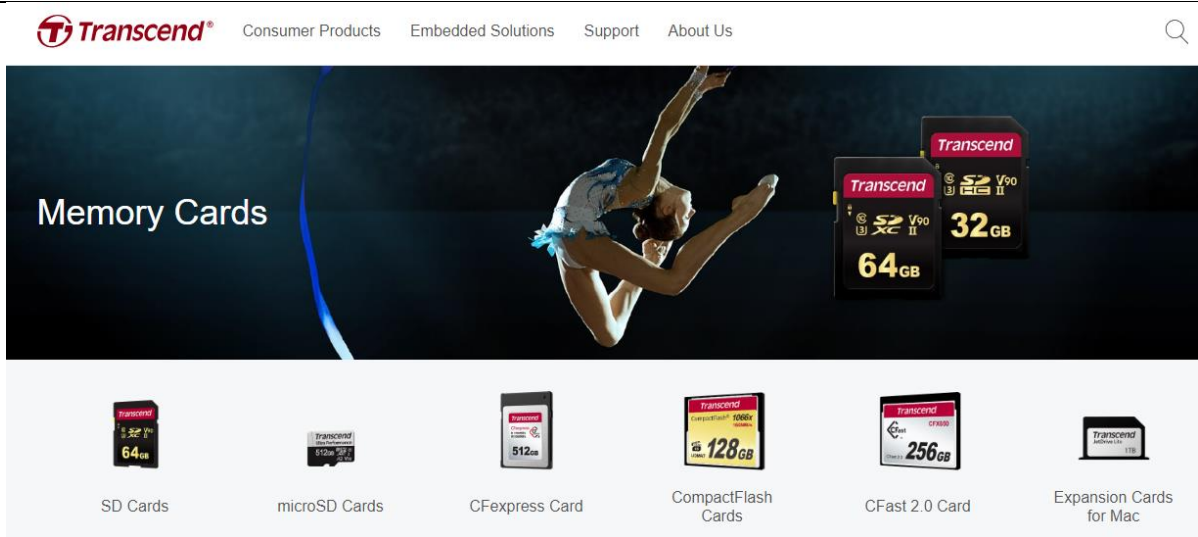
Appendix A: Claim Chart for U.S. Patent 8,977,783

	Step 1: Put the memory card into the reader.  Find the correct adapter on your reader and put your memory card into the reader. USB-A readers can have many kinds of adapters built into the one unit. EBS sells 3 models of USB-A readers. The R3 is a USB 3.0 reader that has both a MicroSD card slot and a full size SD card slot. This is great! You can convert both major kinds of memory card to USB-A with this reader to work with your computer. Source: https://bulkmemorycards.com/how-to-use-an-sd-adapter-with-pictures/ Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
7[Pre]. A method of quickly and securely transferring media files from a kiosk to a secure digital (SD) card, the method comprising:	The Transcend Accused Products infringe directly and/or indirectly by performing, inducing others to perform, and/or contributing to the performance of: a method of quickly and securely transferring media files from a kiosk to a secure digital (SD) card. This is a non-limiting preamble. This element is infringed literally, or in the alternative, under the doctrine of equivalents.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system that practices the method of this claim with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system that performs the method of this claim. This element is directly infringed by Transcend through its use, testing, troubleshooting, and demonstration of use to its customers in the United States. This claim is indirectly infringed by users of the Transcend Accused Products as directed by Transcend. For example, as shown below, Transcend manufactures memory cards such as SD cards, microSD cards etc. with different memory categories for the allowing the transferring of media files. The Transcend Accused Products, including microSDHC Class 10 cards are compatible with kiosks (<i>e.g.</i>, DV recorders, mobile phones, personal computers, etc.). The kiosks can use the SD cards by inserting it into the SD card slots. For example, as shown below, Transcend's micro Secure Digital High Capacity (SDHC) cards allows a very high-performance speed (<i>e.g.</i>, up to 24 Mbps for reading data and up to 22 Mbps for writing data) for transferring of media files. These microSDHC cards are CPRM (Content Protection for Recorded media) compliant, which is important for content or media security. The CPRM technology allows secure transferring of the file from a kiosk to the SDHC memory cards. For example, Transcend microSDHC cards are designed for use in mobile phones, personal computers and other small devices by storing the media files, documents or applications, etc. The storage is done either by inserting the card in the slot of the mobile phones or by externally connecting the SD card in the personal computer USB slots or adapter slot.
--	---

Appendix A: Claim Chart for U.S. Patent 8,977,783

	 Source: https://www.transcend-info.com/product/memory-card USDC10M The ideal choice for small form factor devices with high performance demands, Transcend's High Capacity microSD cards are specifically designed for use in digital cameras, DV recorders, mobile phones, and other small devices. To ensure reliability and endurance, these microSD cards are manufactured using brand-name MLC NAND Flash chips and undergo extensive reliability testing at all stages of production.
--	--

Appendix A: Claim Chart for U.S. Patent 8,977,783

	<table><tr><td data-bbox="688 191 1812 529"> Performance <table><tr><td>Read Speed (Max.)</td><td>Up to 24 MB/s</td></tr><tr><td>Write Speed (Max.)</td><td>Up to 22 MB/s</td></tr><tr><td>Terabytes Written (TBW)</td><td>Up to 60 TBW</td></tr><tr><td>Note</td><td> • Speed may vary due to host hardware, software, usage, and storage capacity. • Terabytes Written (TBW) expresses the endurance under the highest capacity. </td></tr></table></td><td data-bbox="791 529 1709 997"> Firmware Features • Built-in ECC (Error Correction Code) functionality • Early Move • Wear-Leveling • Supports Content Protection for Recorded Media (CPRM) • Supports password protection and secure erase via Scope Pro • Power-saving partial and slumber modes • Power-saving auto-standby and power-off modes </td></tr><tr><td colspan="2" data-bbox="569 997 1929 1107">Source: https://www.transcend-info.com/Embedded/Products/No-585</td></tr></table>	Performance <table><tr><td>Read Speed (Max.)</td><td>Up to 24 MB/s</td></tr><tr><td>Write Speed (Max.)</td><td>Up to 22 MB/s</td></tr><tr><td>Terabytes Written (TBW)</td><td>Up to 60 TBW</td></tr><tr><td>Note</td><td> • Speed may vary due to host hardware, software, usage, and storage capacity. • Terabytes Written (TBW) expresses the endurance under the highest capacity. </td></tr></table>	Read Speed (Max.)	Up to 24 MB/s	Write Speed (Max.)	Up to 22 MB/s	Terabytes Written (TBW)	Up to 60 TBW	Note	• Speed may vary due to host hardware, software, usage, and storage capacity. • Terabytes Written (TBW) expresses the endurance under the highest capacity.	Firmware Features • Built-in ECC (Error Correction Code) functionality • Early Move • Wear-Leveling • Supports Content Protection for Recorded Media (CPRM) • Supports password protection and secure erase via Scope Pro • Power-saving partial and slumber modes • Power-saving auto-standby and power-off modes	Source: https://www.transcend-info.com/Embedded/Products/No-585	
Performance <table><tr><td>Read Speed (Max.)</td><td>Up to 24 MB/s</td></tr><tr><td>Write Speed (Max.)</td><td>Up to 22 MB/s</td></tr><tr><td>Terabytes Written (TBW)</td><td>Up to 60 TBW</td></tr><tr><td>Note</td><td> • Speed may vary due to host hardware, software, usage, and storage capacity. • Terabytes Written (TBW) expresses the endurance under the highest capacity. </td></tr></table>	Read Speed (Max.)	Up to 24 MB/s	Write Speed (Max.)	Up to 22 MB/s	Terabytes Written (TBW)	Up to 60 TBW	Note	• Speed may vary due to host hardware, software, usage, and storage capacity. • Terabytes Written (TBW) expresses the endurance under the highest capacity.	Firmware Features • Built-in ECC (Error Correction Code) functionality • Early Move • Wear-Leveling • Supports Content Protection for Recorded Media (CPRM) • Supports password protection and secure erase via Scope Pro • Power-saving partial and slumber modes • Power-saving auto-standby and power-off modes				
Read Speed (Max.)	Up to 24 MB/s												
Write Speed (Max.)	Up to 22 MB/s												
Terabytes Written (TBW)	Up to 60 TBW												
Note	• Speed may vary due to host hardware, software, usage, and storage capacity. • Terabytes Written (TBW) expresses the endurance under the highest capacity.												
Source: https://www.transcend-info.com/Embedded/Products/No-585													

Appendix A: Claim Chart for U.S. Patent 8,977,783

	Ready for the Secured Digital Content Content Protection for Recordable Media (CPRM), the content protection technology used for SD standards, is key to enabling a distribution system for music, video, etc. CPRM provides a high level of protection against illegal copying. The content protection technology was developed by the 4C Entity, LLC, The digital contents copyright protection technology licensing organization of IBM, Intel, Panasonic, and Toshiba. The SD memory card CPRM function has the following features: ▪ Success of mutual authentication enables host to access card protected area. ▪ The protected area consumes small memory area because a content key is supposed to be saved instead of a large content. ▪ Revocation feature can prevent a specific host from accessing card protected area. ▪ SD CPRM Host Devices can playback an encrypted content mutually that is stored in an SD memory card. Source: https://www.sdcard.org/developers/sd-standard-overview/content-protection/
7[a]. identifying a media file for download to the SD card;	Each Accused Product performs the method of identifying a media file for download to the SD card. This element is infringed literally, or in the alternative, under the doctrine of equivalents. <i>See supporting evidence for claim 1[a].</i> Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system of this claim. This element is directly infringed by Transcend through its use, testing, troubleshooting, and demonstration of use to its customers in the United States. This claim is indirectly infringed by users of the Transcend Accused Products as directed by Transcend.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	For example, as shown below, a user can identify a media file to be moved or copied to the external storage device, such as an SD card. Back up files from your current PC to an external storage device 1. Connect your external storage device to your current Windows 11 PC. 2. On the taskbar, select File Explorer . 3. Locate the files you wish to copy, or the folders where those files are stored. 4. To copy multiple files, hold CTRL as you select additional files or folders. 5. Once you have files and folders highlighted, select and hold (or right-click) the folders, then select Show more options > Send to. Select your external storage device name from the list of options. 6. Your files and folders will begin copying to your drive. You may need to repeat steps 3 – 5 if you have files stored in multiple locations. Make sure to also move files from locations like your Documents, Desktop, Downloads, Favorites, Music, Podcasts, Pictures, and Videos folders. Source: https://support.microsoft.com/en-us/windows/move-your-files-to-a-new-windows-pc-using-an-external-storage-device-dd139b2e-bc73-4431-8e6e-c96e10dffdf5 Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
7 [b] . pre-allocating space on the SD card for a playable content portion of the media file, wherein the playable content portion of the media file is encrypted	Each Accused Product performs a method of pre-allocating space on the SD card for a playable content portion of the media file, wherein the playable content portion of the media file is encrypted by a content key that is encrypted by a user key. This element is infringed literally, or in the alternative, under the doctrine of equivalent

Appendix A: Claim Chart for U.S. Patent 8,977,783

by a content key that is encrypted by a user key;	Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system that practices the method of this claim with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system that performs the method of this claim. This element is directly infringed by Transcend through its use, testing, troubleshooting, and demonstration of use to its customers in the United States. This claim is indirectly infringed by users of the Transcend Accused Products as directed by Transcend. <i>See supporting evidence for claim 1[f].</i> For example, as shown below, a media file processing module prepares media files and metadata files to be written to the SD card in secure and unsecure areas. Logical locations of CPRM components are defined for the “SD memory card”. As per the figures, a pre-allocated space on the SD card (<i>e.g.</i>, user data area) is defined for the encrypted content / files (playable content of the media file). The corresponding playable media content is encrypted using a series of keys. 3.3 CPRM Components This section describes the logical location and format of the CPRM components, when stored on the "SD Memory Card." Figure 3-1 depicts the logical locations of CPRM Components on the "SD Memory Card." These logical locations are used, unless explicitly noted otherwise in an application specific part of <i>CPRM SD Memory Card Book</i>.
--	---

Appendix A: Claim Chart for U.S. Patent 8,977,783

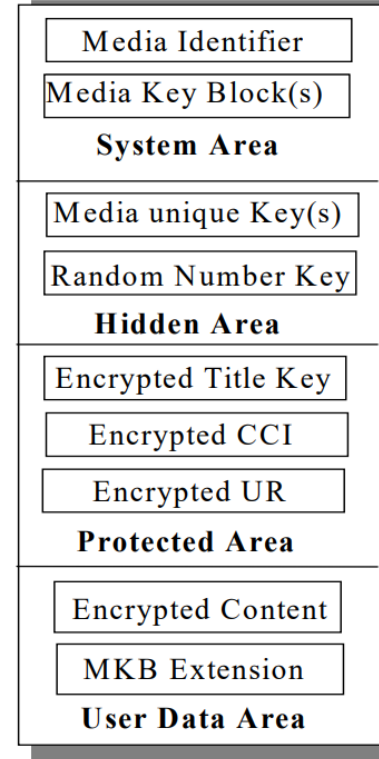


Figure 3-1 – SD Memory Card

- A Media Identifier (ID_{media}) and sixteen Media Key Blocks are pre-recorded in the System Area.
- Sixteen Media Unique Keys and Random Number Key are pre-recorded in the Hidden Area.
- Encrypted Title Keys, Encrypted CCI (Copy Control Information) and Encrypted UR (Usage Rules) are recorded in the Protected Area.
- Encrypted Content and MKB Extension are recorded in the User Data Area

Source: <http://www.4centity.com/document.aspx?doc=2ef45977-c7fd-45f5-b2bf-759ac88764d3>

Appendix A: Claim Chart for U.S. Patent 8,977,783

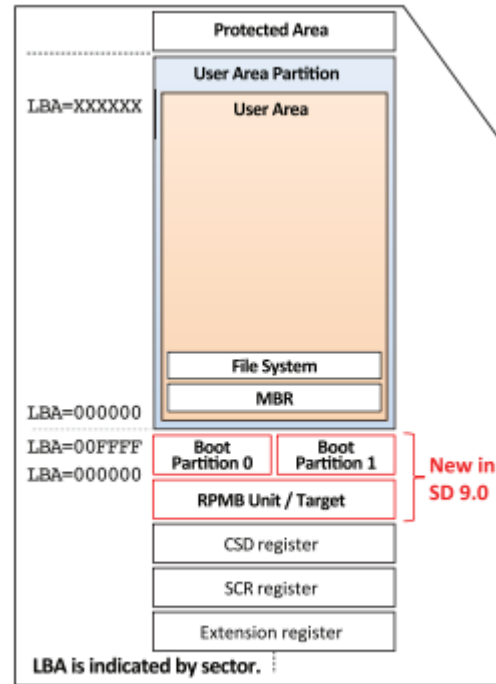


Figure 1-1

Newly added memory structure for Boot and RPMB

Source: <https://www.sdcard.org/cms/wp-content/uploads/2022/05/Boot-TCG-and-RPMB-The-New-Security-Featu-res-Introduced-in-SD-9.0.pdf>

In an SD Memory Card, two kinds of key are stored. One is called a content key which is used to encrypt corresponding content. The other is called a User Key which is used to protect the Content Key values and its usage rules. These keys can be also delivered separately. An example of separate distribution is drawn in Figure 3-1.

Source: <https://www.sdcard.org/cms/wp-content/uploads/2022/05/Boot-TCG-and-RPMB-The-New-Security-Featu-res-Introduced-in-SD-9.0.pdf>

Appendix A: Claim Chart for U.S. Patent 8,977,783

	3.6.1.1 ASF File Encryption SD-Video application treats the Microsoft's Advanced Systems Format (ASF) file as one of the file format that contains video stream. The ASF file is encrypted by the Title Key as follows: • The ASF file consists of an ASF Header Section, ASF Data Section Object (fixed to 50 bytes) and multiple ASF Data Packets. • The ASF Header Section and the ASF Data Section Object are not encrypted. • Each ASF Data Packet consists of a header part (variable size M: less than or equal to 40 bytes) and a data part (variable size N). Size of Data Packet is less than 2^{32} bytes. • Each ASF Data Packet is encrypted by the corresponding Title Key using C2_ECBC (the C2 cipher algorithm in C-CBC mode) as follows. • Each ASF Data Packet starts a new C-CBC cipher chain. • Forty (40) bytes from the top of each ASF Data Packet is not encrypted • The residual data part is encrypted. The last residual block, if it is less than 8 bytes, is not encrypted. Source: http://www.4centity.com/document.aspx?doc=d1aa7cfa-4541-4fb4-a46c-ae030413b Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
7[c]. writing all directory blocks of the playable content portion of the media file together and, thereafter in time, writing all data blocks sequentially of the playable content portion of the media file; and	Each Accused Product performs a method of writing all directory blocks of the playable content portion of the media file together and, thereafter in time, writing all data blocks sequentially of the playable content portion of the media file. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system that practices the method of this claim with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system that performs the method of this claim. This element is directly infringed by Transcend through its use, testing, troubleshooting, and demonstration of use to its customers in the United States. This claim is indirectly infringed by users of the Transcend Accused Products as directed by Transcend.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	<i>See supporting evidence for claim 1[f].</i> For example, as shown below, during the writing process of large media files on the SDHC memory card, a writable space is allocated, called as “directory blocks”. These blocks can be written together (<i>e.g.</i> allocated at once) while writing on the memory card. The directory blocks for all the media content can be written (<i>e.g.</i>, allocated) in the first stage, all at once as depicted in the image below. These directory blocks can be followed by the data blocks containing the encrypted content of the media file. Multiple data blocks are pointed by each directory block and can be arranged sequentially or in a regular serial number. For example, the respective directories (<i>e.g.</i>, PRG001, PRG003, etc.) can be allocated together at the same time. The media content (<i>e.g.</i>, data blocks, such as MOV00X.SFX, MOV00X.SMX, etc.) can be encrypted sequentially, having a serial number for each of the data blocks.
--	---

Appendix A: Claim Chart for U.S. Patent 8,977,783

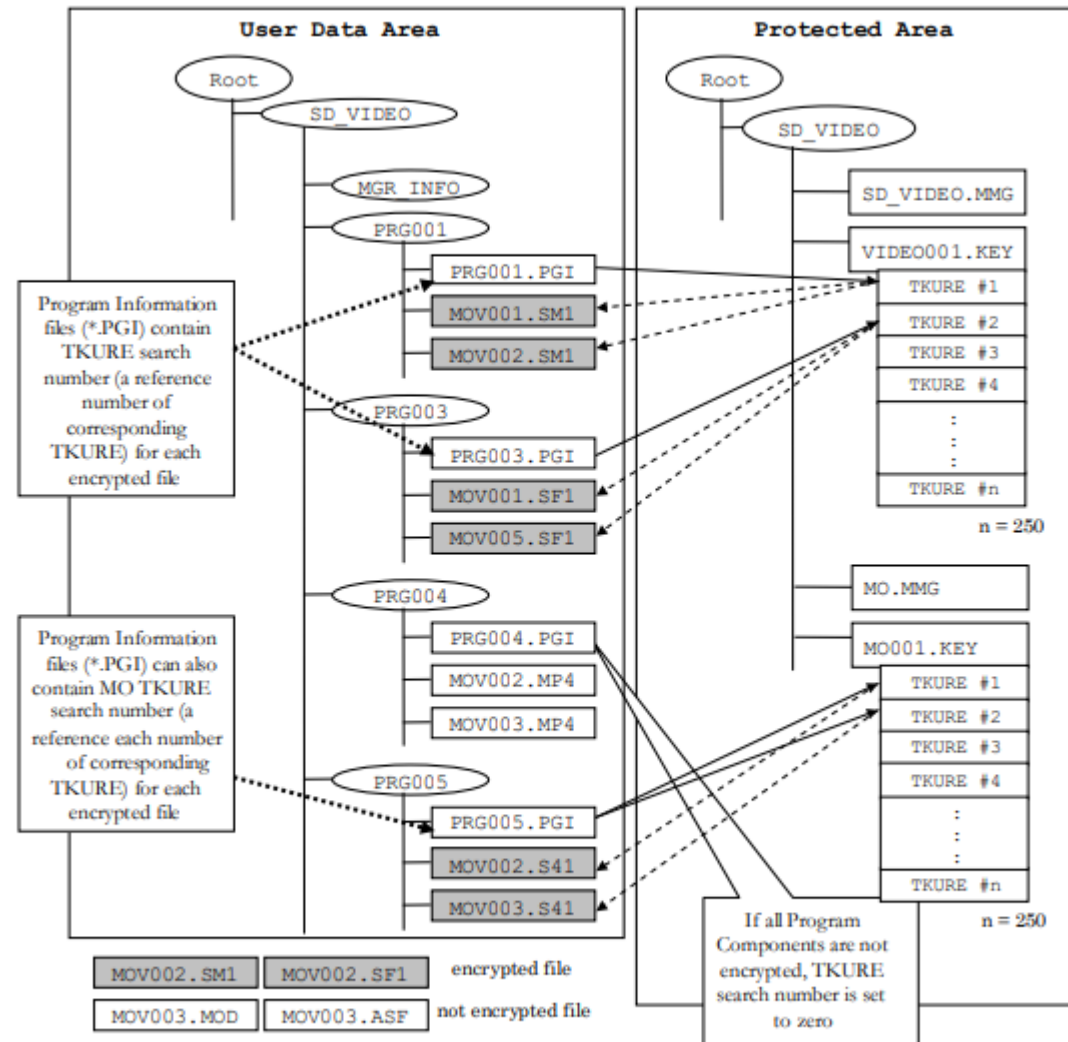


Figure 3-4 Relationship between Directory and Filename

Source: <http://www.4centity.com/document.aspx?doc=d1aa7cfa-4541-4fb4-a46c-ae030413bc4>

Appendix A: Claim Chart for U.S. Patent 8,977,783

	Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
7[d]. writing all data that is to be written to an unsecure area of the SD card, including the encrypted playable content, prior in time to writing any data to a secure area of the SD card, except for the user key.	Each Accused Product performs a method of writing all data that is to be written to an unsecure area of the SD card, including the encrypted playable content, prior in time to writing any data to a secure area of the SD card, except for the user key. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system that practices the method of this claim with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system that performs the method of this claim. This element is directly infringed by Transcend through its use, testing, troubleshooting, and demonstration of use to its customers in the United States. This claim is indirectly infringed by users of the Transcend Accused Products as directed by Transcend. <i>See supporting evidence for claim 1[f] and claim 7[c].</i> For example, as shown below, during encryption of the content, the media unique key which is generated by the media key and the media ID, is used for the encryption of Title key and Usage rules which is encrypted and further decrypted (C2_DCBC) using a session key (Ks). 3.3.4 User Data Area The SD Memory Card shall contain a User Data Area, which is a user-accessible read/write area that is used to store Encrypted content. User Data Area may also contain other user data. When the SD Memory Card is connected to a PC, the user data area typically looks like a normal disk. 3.3.4.1 Encrypted content In the SD Memory Card, each piece of content to be protected shall be encrypted with a unique Title Key, and stored as an encrypted file in the User Data Area. The file system of the User Data Area is typically a FAT12, FAT16, FAT32 or exFAT file system. The directory structure and file names of the encrypted content are defined in each application specific part of the <i>CPRM SD Memory Card Book</i>.

Appendix A: Claim Chart for U.S. Patent 8,977,783

Source: <http://www.4centity.com/document.aspx?doc=2ef45977-c7fd-45f5-b2bf-759ac88764d3>

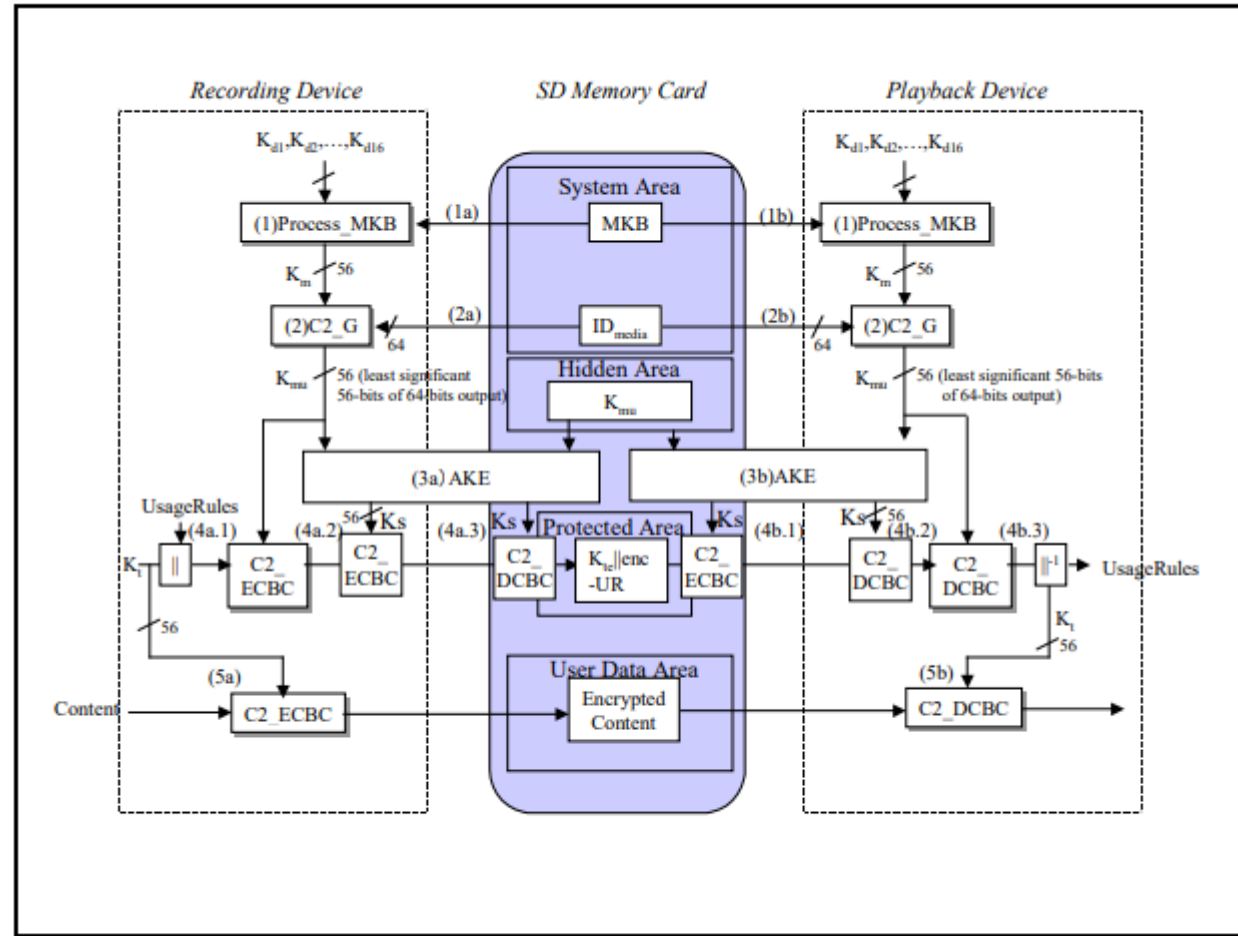


Figure 3-1 Content Encryption and Decryption on SD Memory Card

Appendix A: Claim Chart for U.S. Patent 8,977,783

	3.6.1.1 ASF File Encryption SD-Video application treats the Microsoft's Advanced Systems Format (ASF) file as one of the file format that contains video stream. The ASF file is encrypted by the Title Key as follows: • The ASF file consists of an ASF Header Section, ASF Data Section Object (fixed to 50 bytes) and multiple ASF Data Packets. • The ASF Header Section and the ASF Data Section Object are not encrypted. • Each ASF Data Packet consists of a header part (variable size M: less than or equal to 40 bytes) and a data part (variable size N). Size of Data Packet is less than 2^{32} bytes. • Each ASF Data Packet is encrypted by the corresponding Title Key using C2_ECBC (the C2 cipher algorithm in C-CBC mode) as follows. Source: http://www.4centity.com/document.aspx?doc=d1aa7cfa-4541-4fb4-a46c-aee030413bc4 -(4a) Title Key and Usage Rule Encryption process. The following steps (4a.1) through (4a.3) describe the Title Key and Usage Rule Encryption Process. When the content is encrypted, a Title Key is picked at random. (4a.1) Encrypt the Title Key and Usage Rule Entry by the Media Unique Key associated with MKB. The Recording Device encrypts the Title Key and Usage Rule Entry (see Table 3-10), as a single 64-byte encryption frame using the Media Unique Key associated with MKB. The encryption algorithm is C2_ECBC (the C2 cipher algorithm in C-CBC mode) which is described in the <i>Introduction and Common Cryptographic Elements</i> book. (4a.2) Encrypt the Title Key and Usage Rule Entry by the Session Key.
--	---

Appendix A: Claim Chart for U.S. Patent 8,977,783

	The Recording Device further encrypts the entire 64-byte Title Key and Usage Rule Entry using the Session Key K_s, which is shared at step (3a), using C2_ECBC. The results (the doubly-encrypted Title Key and Usage Rules) are sent to the SD Memory Card. (4a.3) Decrypt the Title Key and Usage Rule Entry by the Session Key. In the SD Memory Card, the doubly-encrypted 64-byte Title Key and Usage Rule Entry is decrypted using the Session Key K_s, which is shared at step (3a). The decryption algorithm is C2_DCBC (the C2 cipher algorithm in C-CBC mode) which is described in the <i>Introduction and Common Cryptographic Elements</i> book. The result (the encrypted Title Key and Usage Rule Entry) is stored in the Protected Area. Source: http://www.4centity.com/document.aspx?doc=d1aa7cfa-4541-4fb4-a46c-ae030413bc4 Each encrypted content file in the User Data Area is associated with the corresponding TKURE for Programs in the Protected Area through its TKURE_SRN for Programs in case of Program Encryption. Source: http://www.4centity.com/document.aspx?doc=d1aa7cfa-4541-4fb4-a46c-ae030413bc4 Note that the Recording Device does not need to write User Key, Content Key and content to an SD Memory Card at a time. For example, there is a case that a Recording Device stores only one User Key and several Content Keys into an SD Memory Card, but does not store the corresponding content data at the time. Source: http://www.4centity.com/document.aspx?doc=868ca775-0fcb-4350-8c19-9860830072d9
--	---

Appendix A: Claim Chart for U.S. Patent 8,977,783

	<pre> graph TD MK[Media Key] -- 56 bit --> C2G[C2_G] MID[Media ID] -- 64 bit --> C2G C2G -- "least significant 56-bits of 64-bits output" --> MUK[Media Unique Key] </pre> Source: http://www.4centity.com/document.aspx?doc=2ef45977-c7fd-45f5-b2bf-759ac88764d3 Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
8. The method of claim 7, wherein, except for a user key, data is only written to the secure area of the SD card if a transaction for the media file successfully completes.	The Transcend Accused Products performs the method of claim 7, wherein, except for a user key, data is only written to the secure area of the SD card if a transaction for the media file successfully completes. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system that practices the method of this claim with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system that performs the method of this claim. This element is directly infringed by Transcend through its use, testing, troubleshooting, and demonstration of use to its customers in the United States. This claim is indirectly infringed by users of the Transcend Accused Products as directed by Transcend. For example, only after the payment is successful, the user can access the content media and download it to the SD memory card. The user key is a unique key required by CPRM for SD cards and is assigned the first time a user transfers content to a particular SD card from the kiosk.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	This is an example of flow to distribute the SD-SD content from a content provider to a user. The SD-SD content distributed by the content provider is encrypted with a content key. The content provider should give a Content ID to both the SD-SD content and the content key. The encrypted SD-SD content would pass through various distribution channels. Network or broadcast may be used and storage media such as CD-ROM or DVD-ROM may be also used. A user would get the encrypted SD-SD content. When the user desires to playback it, the user would take a transaction to buy the right of accessing the SD-SD content. Likely the transaction would include a payment. Then the user would download the content key to access the SD-SD content and store it to an SD Memory Card. When playing it back, the player will search both the encrypted content data and corresponding content key by matching content IDs, then the player can decrypt the SD-SD content and playback it. In an SD Memory Card, two kinds of key are stored. One is called a content key which is used to encrypt corresponding content. The other is called a User Key which is used to protect the Content Key values and its usage rules. These keys can be also delivered separately. An example of separate distribution is drawn in Figure 3-1. Source: http://www.4centity.com/document.aspx?doc=868ca775-0fcb-4350-8c19-9860830072d9 Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
9. The method of claim 7, wherein the SD card is pre-configured with the user key stored in the secure area of the SD card.	Each Accused Product performs the method of claim 7, wherein the SD card is pre-configured with the user key stored in the secure area of the SD card. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system that practices the method of this claim with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system that performs the method of this claim. This element is directly infringed by Transcend through its use, testing, troubleshooting, and demonstration of use to its customers in the United States. This claim is indirectly infringed by users of the Transcend Accused Products as directed by Transcend. <i>See supporting evidence for claim element 7[d].</i>

Appendix A: Claim Chart for U.S. Patent 8,977,783

	Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
10. The method of claim 7, further comprising: writing the user key to the secure area of the SD card prior in time to writing all data to the unsecure area of the SD card; and writing other data to the secure area of the SD card after in time writing all data to the unsecure area of the SD card.	Each Accused Product performs the method of claim 7, further comprising: writing the user key to the secure area of the SD card prior in time to writing all data to the unsecure area of the SD card and writing other data to the secure area of the SD card after in time writing all data to the unsecure area of the SD card. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system that practices the method of this claim with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system that performs the method of this claim. This element is directly infringed by Transcend through its use, testing, troubleshooting, and demonstration of use to its customers in the United States. This claim is indirectly infringed by users of the Transcend Accused Products as directed by Transcend. <i>See supporting evidence for claim element 7[d].</i> Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
11. The method of claim 7, where the directory blocks are optionally written at once.	Each Accused Product performs the method of claim 7, where the directory blocks are optionally written at once. This element is infringed literally, or in the alternative, under the doctrine of equivalents. Transcend induces infringement and contributes to the infringement of its customers and end users by providing components of the system that practices the method of this claim with no substantial non-infringing uses, as well as directing its customers and end users to put into use the system that performs the method of this claim. This element is directly infringed by Transcend through its use, testing, troubleshooting, and demonstration of use to its customers in the United States. This claim is indirectly infringed by users of the Transcend Accused Products as directed by Transcend.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	Upon information and belief, directory blocks can be written sequentially and/or optionally written at once. <i>See supporting evidence for claim element 7[c].</i> Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
12[Pre]. A non-transitory computer readable storage medium storing instruction thereon, the instructions when executed cause at least one processor to:	The Transcend Accused Products infringe directly and/or indirectly by providing a system comprising: a non-transitory computer readable storage medium storing instruction thereon, the instructions when executed causing at least one processor to perform the method. This is a non-limiting preamble. This element is infringed literally, or in the alternative, under the doctrine of equivalents. For example, as shown below, a kiosk (<i>e.g.</i>, laptop) comes with a non-transitory computer readable storage medium (<i>e.g.</i>, storage medium) and a processor. A laptop's specifications can make a big difference in its performance, so it's essential to be informed. Choosing the correct specifications for your laptop can significantly enhance its performance and user-friendliness. Shopping for a new laptop can be overwhelming, especially when understanding all the technical specifications. Here's a quick rundown of the important factors to consider before purchasing. Processors Just like the human brain, the central processing unit, also known as the CPU, is a computer's control centre, directing all the other components to work together seamlessly. The market offers a diverse range of CPUs, each with its unique merits and demerits. Intel® Core™ i3, i5, i7, and i9 CPUs and the AMD Ryzen™ series stand among the most sought-after CPU types. The key factor that sets apart different CPU types is their number of cores. A core is a solitary processor capable of performing instructions. Increased core count in CPUs can lead to greater multitasking capability and augment performance, potentially boosting speed. CPU performance can be affected by factors beyond clock speed, including cache memory size and architecture type. The clock speed is the rate at which the CPU operates, and cache memory is a small quantity of memory that the CPU can access quickly. Different tasks may require different architectures to utilize the CPU's potential fully.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	RAM RAM, also known as random access memory, is a computer's temporary storage for data. It retains the data that your computer is presently utilizing, including the applications you have running and the documents you are working on. With increased RAM, the computer can store more data in its short-term memory and retrieve it quickly, thus boosting performance. Storage While hard disk drive (HDD) and solid-state drive (SSD) are storage devices, their storage media and operational mechanisms differ. Magnetic platters are used in HDDs to store data, whereas flash memory is used in SSDs. This difference in technology directly impacts the overall performance and cost. Source: https://www.hp.com/in-en/shop/tech-takes/post/laptop-specifications-for-home
12[a]. identify a media file for download to an SD card;	Each Accused Product comprises a processor to identify a media file for download to an SD card. This element is infringed literally, or in the alternative, under the doctrine of equivalents. <i>See supporting evidence for claim element 7[a].</i> Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
12[b]. pre-allocate space on the SD card for a playable content portion of the media file, wherein the playable content portion of the media file is encrypted by a content key that is encrypted by a user key;	Each Accused Product comprises a processor to pre-allocate space on the SD card for a playable content portion of the media file, wherein the playable content portion of the media file is encrypted by a content key that is encrypted by a user key. This element is infringed literally, or in the alternative, under the doctrine of equivalents. <i>See supporting evidence for claim element 7[b].</i> Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
12[c]. write all directory blocks together of the playable content portion of the media file and, thereafter in time, write all data blocks sequentially of	Each Accused Product comprises a processor to write all directory blocks together of the playable content portion of the media file and, thereafter in time, write all data blocks sequentially of the playable content portion of the media file. This element is infringed literally, or in the alternative, under the doctrine of equivalents.

Appendix A: Claim Chart for U.S. Patent 8,977,783

the playable content portion of the media file; and	<i>See supporting evidence for claim element [7c].</i> Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
12[d]. write all data that is to be written to an unsecure area of the SD card, including the encrypted playable content, prior in time to writing any data to a secure area of the SD card, except for the user key.	Each Accused Product comprises a processor to write all data that is to be written to an unsecure area of the SD card, including the encrypted playable content, prior in time to writing any data to a secure area of the SD card, except for the user key. This element is infringed literally, or in the alternative, under the doctrine of equivalents. <i>See supporting evidence for claim element 7[d].</i> Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
13. The computer readable storage medium of claim 12, wherein, except for a user key, data is only written to the secure area of the SD card if a transaction for the media file successfully completes.	Each Accused Product comprises the computer readable storage medium of claim 12, wherein, except for a user key, data is only written to the secure area of the SD card if a transaction for the media file successfully completes. This element is infringed literally, or in the alternative, under the doctrine of equivalents. <i>See supporting evidence for claim 8.</i> Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
14. The computer readable storage medium of claim 12, wherein the SD card is pre-configured with the user key stored in the secure area of the SD card.	Each Accused Product comprises the computer readable storage medium of claim 12, wherein the SD card is pre-configured with the user key stored in the secure area of the SD card. This element is infringed literally, or in the alternative, under the doctrine of equivalents. <i>See supporting evidence for claim 7[d] and claim 9.</i> Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.

Appendix A: Claim Chart for U.S. Patent 8,977,783

15. The computer readable storage medium of claim 12, further comprising instructions that when executed cause the at least one processor to: write the user key to the secure area of the SD card prior in time to a write of all data to the unsecure area of the SD card; and write other data to the secure area of the SD card after in time a write of all data to the unsecure area of the SD card.	Each Accused Product comprises the computer readable storage medium of claim 12, further comprising instructions that when executed cause the at least one processor to: write the user key to the secure area of the SD card prior in time to a write of all data to the unsecure area of the SD card; and write other data to the secure area of the SD card after in time a write of all data to the unsecure area of the SD card. This element is infringed literally, or in the alternative, under the doctrine of equivalents. <i>See supporting evidence for claim element 7[d].</i> Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
16. The computer readable storage medium of claim 12, where the directory blocks are optionally written at once.	Each Accused Product comprises the computer readable storage medium of claim 12, where the directory blocks are optionally written at once. This element is infringed literally, or in the alternative, under the doctrine of equivalents. <i>See supporting evidence for claim 7[c] and claim 11.</i> Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
17. The computer readable storage medium of claim 12 wherein the instructions cause the media file to be downloaded to the SD card in substantially 2 minutes.	Each Accused Product comprises the computer readable storage medium of claim 12 wherein the instructions cause the media file to be downloaded to the SD card in substantially 2 minutes. This element is infringed literally, or in the alternative, under the doctrine of equivalents. For example, as shown below, the Transcend Accused Products including the microSDHC Class 10 causes the media file to be downloaded to the SD card in substantially 2 minutes.

Appendix A: Claim Chart for U.S. Patent 8,977,783

	USDC10M The ideal choice for small form factor devices with high performance demands, Transcend's High Capacity microSD cards are specifically designed for use in digital cameras, DV recorders, mobile phones, and other small devices. To ensure reliability and endurance, these microSD cards are manufactured using brand-name MLC NAND Flash chips and undergo extensive reliability testing at all stages of production. Performance <table><tr><td>Read Speed (Max.)</td><td>Up to 24 MB/s</td></tr><tr><td>Write Speed (Max.)</td><td>Up to 22 MB/s</td></tr><tr><td>Terabytes Written (TBW)</td><td>Up to 60 TBW</td></tr><tr><td>Note</td><td> - Speed may vary due to host hardware, software, usage, and storage capacity. - Terabytes Written (TBW) expresses the endurance under the highest capacity. </td></tr></table> Source: https://www.transcend-info.com/Embedded/Products/No-585 Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.	Read Speed (Max.)	Up to 24 MB/s	Write Speed (Max.)	Up to 22 MB/s	Terabytes Written (TBW)	Up to 60 TBW	Note	- Speed may vary due to host hardware, software, usage, and storage capacity. - Terabytes Written (TBW) expresses the endurance under the highest capacity.
Read Speed (Max.)	Up to 24 MB/s								
Write Speed (Max.)	Up to 22 MB/s								
Terabytes Written (TBW)	Up to 60 TBW								
Note	- Speed may vary due to host hardware, software, usage, and storage capacity. - Terabytes Written (TBW) expresses the endurance under the highest capacity.								
18. The method of claim 7 wherein the media file is downloaded to the SD card in substantially 2 minutes.	Each Accused Product performs the method of claim 7 wherein the media file is downloaded to the SD card in substantially 2 minutes. This element is infringed literally, or in the alternative, under the doctrine of equivalents.								

Appendix A: Claim Chart for U.S. Patent 8,977,783

	This element is directly infringed by Transcend through its use, testing, troubleshooting, and demonstration of use to its customers in the United States. This claim is indirectly infringed by users of the Transcend Accused Products as directed by Transcend. <i>See supporting evidence for claim 17.</i> Truesight reserves its right to identify source code under Local Rule 3-1 and the Court's Standing Proposed Discovery Order Section 3(a)(i) once access to relevant source code is provided.
--	---