

**UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

AIRE TECHNOLOGY LTD.,

Plaintiff,

v.

GOOGLE LLC,

Defendant.

Case No. 6:21-cv-01104

JURY TRIAL DEMANDED

**COMPLAINT FOR PATENT INFRINGEMENT
AGAINST GOOGLE LLC**

This is an action for patent infringement arising under the Patent Laws of the United States of America, 35 U.S.C. § 1 *et seq.*, in which Plaintiff Aire Technology Limited (“Plaintiff” or “Aire”) makes the following allegations against Defendant Google LLC (“Defendant” or “Google”):

INTRODUCTION

1. This complaint arises from Google’s unlawful infringement of the following United States patents owned by Plaintiff, which relate to improvements in Near Field Communication (NFC) and secure digital payment solutions: United States Patent Nos. 8,581,706 (“the ’706 Patent”), 8,816,827 (“the ’827 Patent”), 8,205,249 (“the ’249 Patent”), and 8,174,360 (“the ’360 Patent”) (collectively, the “Asserted Patents”).

PARTIES

2. Plaintiff Aire Technology Limited is a limited liability company organized and existing under the law of Ireland, with its principal place of business at The Hyde Building, Suite 23, The Park, Carrickmines, Dublin 18, Ireland. Aire is the sole owner by assignment of all rights,

title, and interest in the Asserted Patents, including the right to recover damages for past, present, and future infringement.

3. On information and belief, Defendant Google LLC is a wholly-owned subsidiary of Alphabet, Inc. and a Delaware limited liability company with a principal place of business at 1600 Amphitheatre Parkway, Mountain View, California 94043. Google may be served with process through its registered agent, the Corporation Service Company dba CSC – Lawyers Incorporating Service Company at 211 East 7th Street, Suite 620, Austin, Texas 78701. Google is registered to do business in the State of Texas and has been since at least November 17, 2006.

JURISDICTION AND VENUE

4. This action arises under the patent laws of the United States, Title 35 of the United States Code. This Court has original subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

5. This Court has personal jurisdiction over Google in this action because Google has committed acts within this District giving rise to this action and has established minimum contacts with this forum such that the exercise of jurisdiction over Google would not offend traditional notions of fair play and substantial justice. Google, directly and through subsidiaries or intermediaries, has committed and continues to commit acts of infringement in this District by, among other things, importing, offering to sell, and selling products that infringe the Asserted Patents.

6. Venue is proper in this District under 28 U.S.C. §§ 1391 and 1400(b). Defendant Google is registered to do business in Texas. Additionally, upon information and belief, Defendant has transacted business in this District and has committed acts of direct and indirect infringement in this District by, among other things, making, using, offering to sell, selling, and importing

products that infringe the Asserted Patents. Google has regular and established places of business in this District, including at 500 West 2nd Street, Austin, Texas 78701.¹ As of June 2019, Google had more than 1,100 employees in Austin.² Google currently has, as of October 2021, over 400 job postings for Austin, Texas.³

THE ASSERTED PATENTS

7. On November 12, 2013, the United States Patent and Trademark Office issued U.S. Patent No. 8,581,706 (“the ’706 Patent”), entitled “Data storage medium and method for contactless communication between the data storage medium and a reader,” after full and fair examination. Plaintiff is the assignee of all rights, title, and interest in and to the ’706 Patent and possesses all rights of recovery under the ’706 Patent, including the right to recover damages for past, present, and future infringement. The ’706 Patent is valid and enforceable. A true and correct copy of the ’706 Patent is attached hereto as Exhibit 1.

8. On August 26, 2014, the United States Patent and Trademark Office issued U.S. Patent No. 8,816,827 (“the ’827 Patent”), entitled “Data storage medium and method for contactless communication between the data storage medium and a reader,” after full and fair examination. Plaintiff is the assignee of all rights, title, and interest in and to the ’827 Patent and possesses all rights of recovery under the ’827 Patent, including the right to recover damages for

¹ See, e.g., <https://www.kvue.com/article/money/economy/boomtown-2040/google-austin-texas-real-estate-report/269-2ce6e60e-e8c3-46f5-aca6-864175e67950>.

² See, e.g., <https://www.bizjournals.com/austin/news/2019/06/14/google-confirms-austin-expansion-will-begin-moving.html#:~:text=Google%20currently%20has%20more%20than,people%20operations%2C%20finance%20and%20marketing>.

³ See <https://careers.google.com/jobs/results/?location=Austin,%20TX,%20USA>.

past, present, and future infringement. The '827 Patent is valid and enforceable. A true and correct copy of the '827 Patent is attached hereto as Exhibit 2.

9. On June 19, 2012, the United States Patent and Trademark Office issued U.S. Patent No. 8,205,249 (“the '249 Patent”), entitled “Method for carrying out a secure electronic transaction using a portable data support,” after full and fair examination. Plaintiff is the assignee of all rights, title, and interest in and to the '249 Patent and possesses all rights of recovery under the '249 Patent, including the right to recover damages for past, present, and future infringement. The '249 Patent is valid and enforceable. A true and correct copy of the '249 Patent is attached hereto as Exhibit 3.

10. On May 8, 2012, the United States Patent and Trademark Office issued U.S. Patent No. 8,174,360 (“the '360 Patent”), entitled “Communication apparatus for setting up a data connection between intelligent devices,” after full and fair examination. Plaintiff is the assignee of all rights, title, and interest in and to the '360 Patent and possesses all rights of recovery under the '360 Patent, including the right to recover damages for past, present, and future infringement. The '360 Patent is valid and enforceable. A true and correct copy of the '360 Patent is attached hereto as Exhibit 4.

GOOGLE’S INFRINGEMENT

11. The allegations provided below are exemplary and without prejudice to Plaintiff’s infringement contentions provided pursuant to the Court’s scheduling order and local rules. Plaintiff’s claim construction contentions regarding the meaning and scope of the claim terms will be provided under the Court’s scheduling order and local rules. As detailed below, each element of at least one claim of each of the Asserted Patents is literally present in the accused products. To the extent that any element is not literally present, each such element is present under the doctrine

of equivalents. Plaintiff's analysis below should not be taken as an admission that the preamble is limiting. While publicly available information is cited below, Plaintiff may rely on other forms of evidence to prove infringement, including evidence that is solely in the possession of Google and/or third parties.

12. The accused products include at least the following products, as well as products with reasonably similar functionality and all 5G, XL, and Pro varieties of these products. Identification of the accused products will be provided in Plaintiff's infringement contentions pursuant to the Court's scheduling order and local rules. Google imports, uses, makes, offers for sale, and sells in the United States the following products that support NFC and/or mobile payment applications, such as Google Pay, that infringe at least one claim of the Asserted Patents: Pixel, Pixel XL, Pixel 2, Pixel 2 XL, Pixel 3, Pixel 3 XL, Pixel 3a, Pixel 3a XL, Pixel 4, Pixel 4 XL, Pixel 4a, Pixel 4a (5G), Pixel 5, Pixel 5a (5G), Pixel 6, and Pixel 6 Pro (the "Accused Products").

COUNT I

INFRINGEMENT OF U.S. PATENT NO. 8,581,706

13. Plaintiff realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

14. Google has been and is now directly infringing the '706 Patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a), including by making, using, selling, and/or offering for sale in the United States or importing into the United States infringing products, including at least the Accused Products identified above. The Accused Products satisfy all of the claim limitations of one or more claims of the '706 Patent, including but not limited to claim 11.

15. Claim 11 of the '706 Patent recites a “contactlessly communicating portable data carrier.” To the extent the preamble is limiting, the Accused Products each include a portable data carrier that is capable of contactless communication through the use of Near Field Communication (NFC) technology. For example, Google advertises that the Accused Products support NFC:

Google Pixel 5a with 5G Overview **Tech Specs** Compare Trade-in & Financing Setup & Tips

Wireless and Location

- Wi-Fi 2.4 GHz + 5 GHz 802.11a/b/g/n/ac 2x2 MIMO
- Bluetooth® v5.0 + LE, A2DP (HD codecs: AptX, AptX HD, LDAC, AAC)
- NFC
- Google Cast

See https://store.google.com/us/product/pixel_5a_5g_specs?hl=en-US.

16. Claim 11 of the '706 Patent recites that the portable data carrier comprises “at least two applications stored thereon.” The Accused Products are configured to store at least two applications. For example, the Accused Products are configured to store at least two applications that utilize NFC:

Service selection

When the user taps a device to an NFC reader, the Android system needs to know which HCE service the NFC reader wants to communicate with. The ISO/IEC 7816-4 specification defines a way to select applications, centered around an Application ID (AID). An AID consists of up to 16 bytes. If you are emulating cards for an existing NFC reader infrastructure, the AIDs that those readers look for are typically well-known and publicly registered (for example, the AIDs of payment networks such as Visa and MasterCard).

If you want to deploy new reader infrastructure for your own application, you must register your own AIDs. The registration procedure for AIDs is defined in the ISO/IEC 7816-5 specification. We recommend registering an AID as per 7816-5 if you are deploying a HCE application for Android, because it avoids collisions with other applications.

AID conflict resolution

Multiple `HostApuService` components may be installed on a single device, and the same AID can be registered by more than one service. Android resolves AID conflicts differently depending on which category an AID belongs to. Each category may have a different conflict resolution policy.

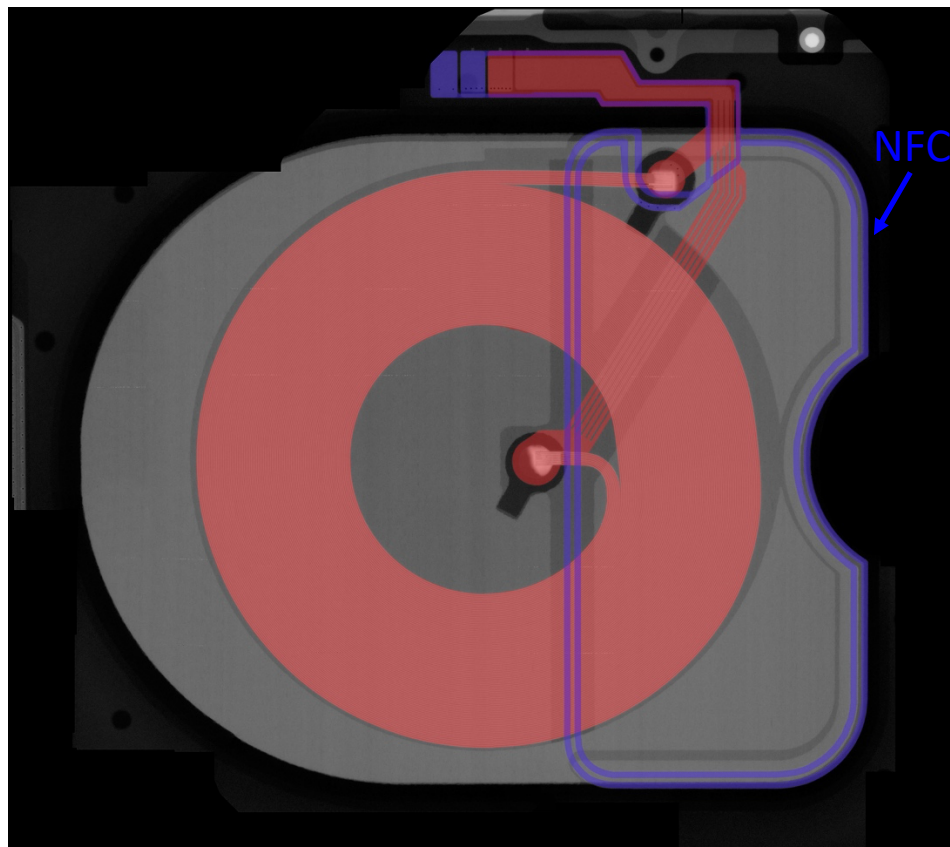
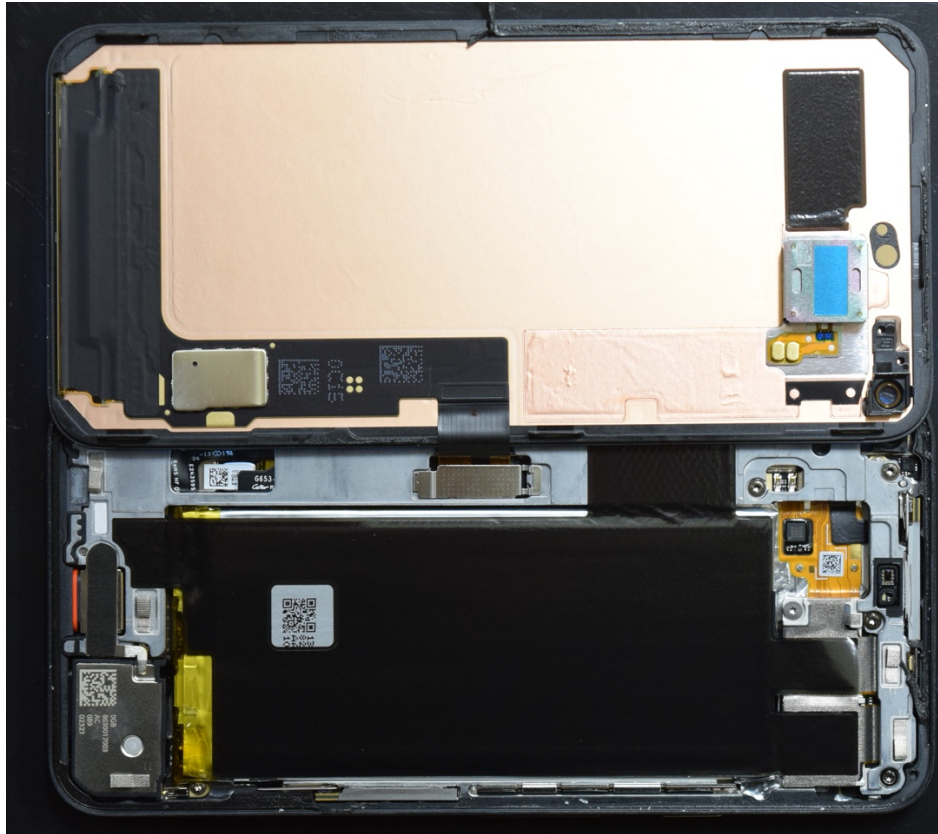
For some categories, such as payment, the user might be able to select a default service in the Android settings UI. For other categories, the policy might be to always ask the user which service to invoke in case of conflict. For information about how to query the conflict resolution policy for a certain category, see `getSelectionModeForCategory()`.

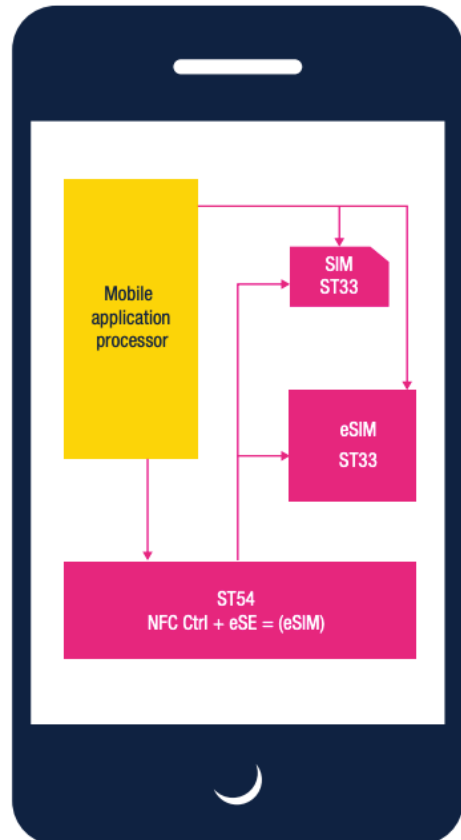
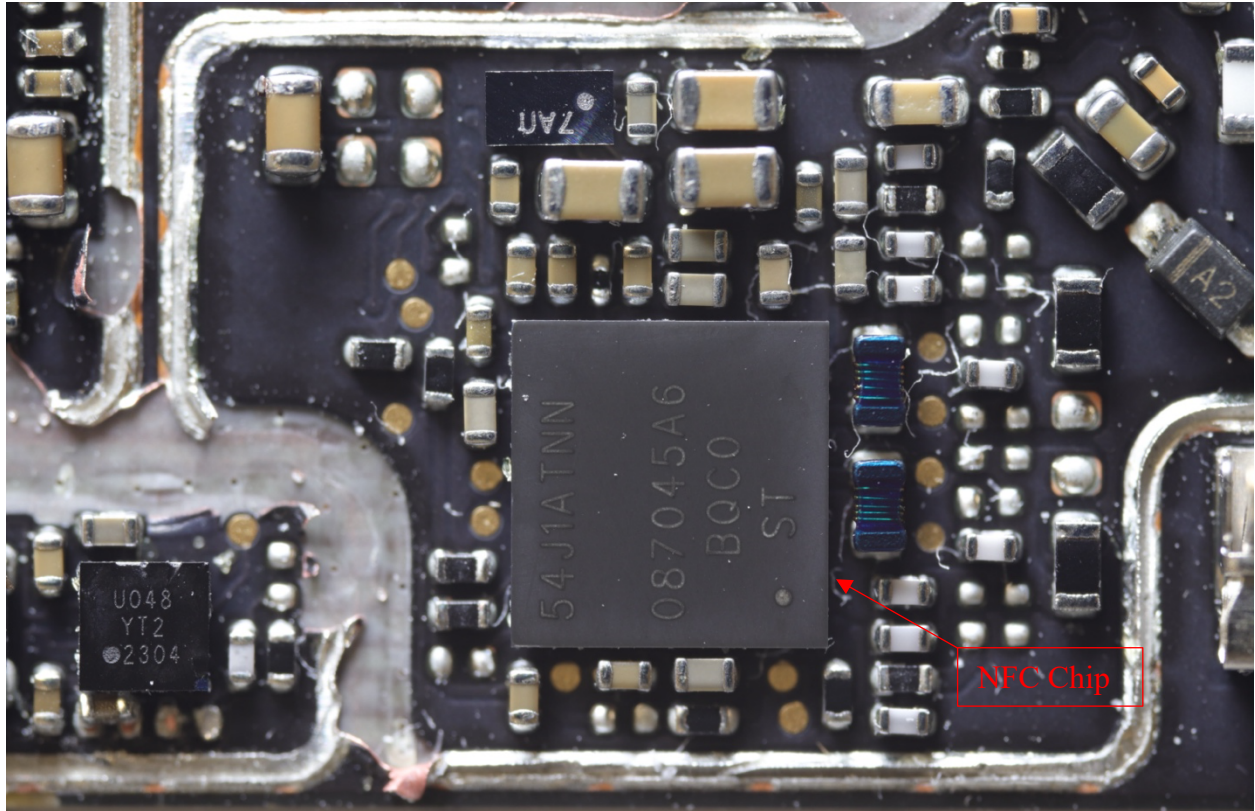
The following is an example of the corresponding `apduservice.xml` file registering two AIDs:

```
<offhost-apdu-service xmlns:android="http://schemas.android.com/apk/res/android"
    android:description="@string/servicedesc">
    <aid-group android:description="@string/subscription" android:category="other">
        <aid-filter android:name="F0010203040506" />
        <aid-filter android:name="F0394148148100" />
    </aid-group>
</offhost-apdu-service>
```

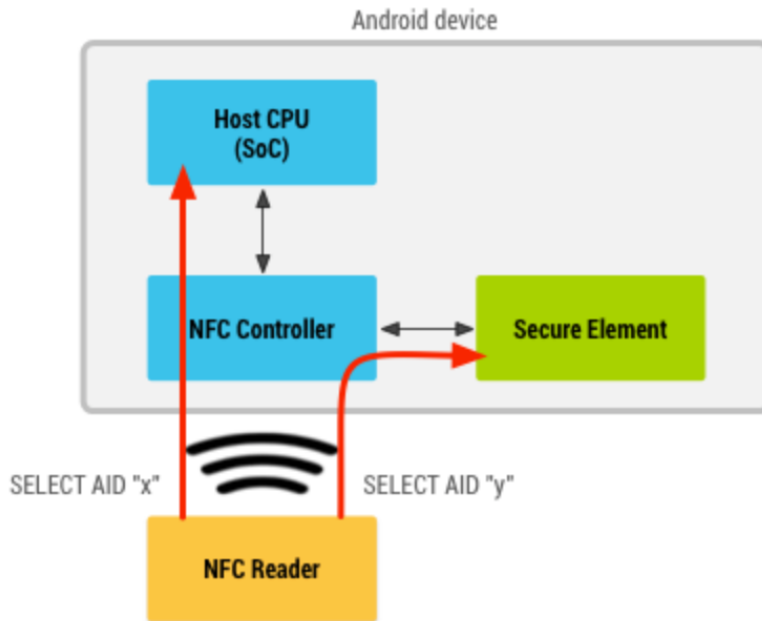
See <https://developer.android.com/guide/topics/connectivity/nfc/hce>.

17. Claim 11 of the '706 Patent recites that the portable data carrier comprises “a communication device configured to control communication between a reading device and the at least two applications.” The Accused Products contain a communication device configured to control communication between a reading device and at least two applications. For example, the Accused Products utilize an NFC antenna, NFC chip, and related hardware and software to control communication with a reading device and at least two applications, as shown in the exemplary Google Pixel 5:





See <https://www.st.com/en/secure-mcus/st54j.html>; see also https://www.emvco.com/wp-content/uploads/approved_products/uploaded/loa/MTA_LOA_GOLL_02519_20Oct20_SHORT.pdf.



See <https://developer.android.com/guide/topics/connectivity/nfc/hce>.

18. Claim 11 of the '706 Patent recites “wherein the communication device is set up to generate communication-readiness signals to the reading device which in each case indicate to the reading device a communication readiness for one of the applications and comprise an identification number assigned to the corresponding communication-readiness application.” The Accused Products contain a communication device that is set up to generate communication-readiness signals to the reading device which in each case indicate to the reading device a communication readiness for one of the applications and comprise an identification number assigned to the corresponding communication-readiness application. For example, the communication device generates communication-readiness signals to an NFC reader which comprise of an Application ID (AID) that corresponds to an application:

Service selection

When the user taps a device to an NFC reader, the Android system needs to know which HCE service the NFC reader wants to communicate with. The ISO/IEC 7816-4 specification defines a way to select applications, centered around an Application ID (AID). An AID consists of up to 16 bytes. If you are emulating cards for an existing NFC reader infrastructure, the AIDs that those readers look for are typically well-known and publicly registered (for example, the AIDs of payment networks such as Visa and MasterCard).

If you want to deploy new reader infrastructure for your own application, you must register your own AIDs. The registration procedure for AIDs is defined in the ISO/IEC 7816-5 specification. We recommend registering an AID as per 7816-5 if you are deploying a HCE application for Android, because it avoids collisions with other applications.

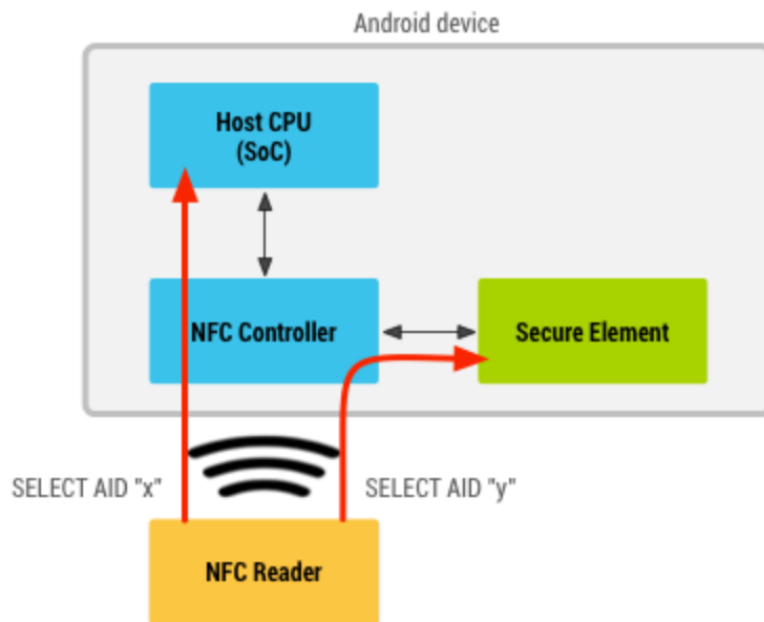
AID conflict resolution

Multiple `HostApuService` components may be installed on a single device, and the same AID can be registered by more than one service. Android resolves AID conflicts differently depending on which category an AID belongs to. Each category may have a different conflict resolution policy.

For some categories, such as payment, the user might be able to select a default service in the Android settings UI. For other categories, the policy might be to always ask the user which service to invoke in case of conflict. For information about how to query the conflict resolution policy for a certain category, see `getSelectionModeForCategory()`.

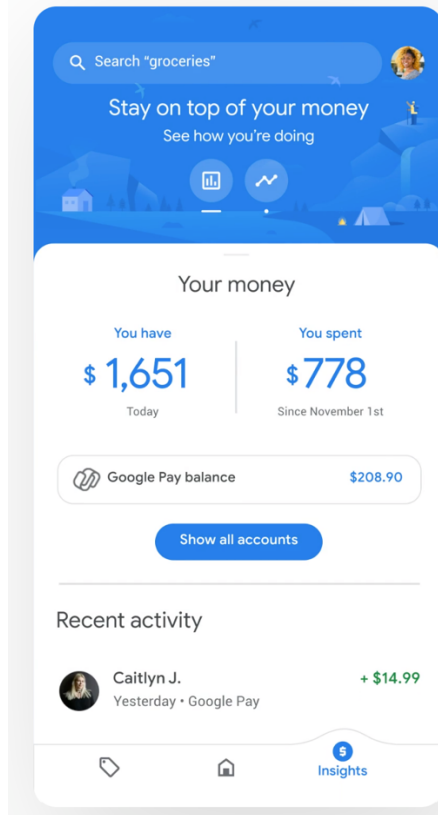
The following is an example of the corresponding `apdu-service.xml` file registering two AIDs:

```
<offhost-apdu-service xmlns:android="http://schemas.android.com/apk/res/android"
    android:description="@string/servicedesc">
  <aid-group android:description="@string/subscription" android:category="other">
    <aid-filter android:name="F0010203040506" />
    <aid-filter android:name="F0394148148100" />
  </aid-group>
</offhost-apdu-service>
```



See <https://developer.android.com/guide/topics/connectivity/nfc/hce>.

19. Claim 11 of the '706 Patent recites “wherein the communication device is set up to store information in a nonvolatile memory of the data carrier about which of the at least two applications last communicated with a reading device.” Each of the Accused Products contains a communication device that is set up to store information in a nonvolatile memory of the data carrier about which of the at least two applications last communicated with a reading device. For example, the Accused Products provide information about the last application that last communicated with a reading device:



Get insights

Learn about your spending patterns and where you can save money.

Sync accounts

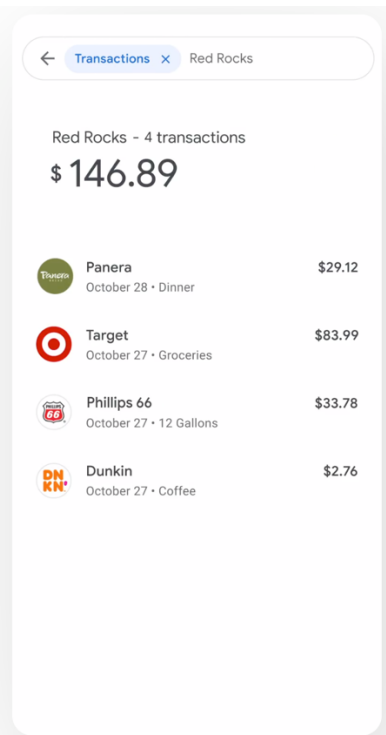
Easily check your balance and spending across all of your linked accounts.

Stay in the know

As money goes in and out, see it reflected in one simple view.

Search your spending the easy way with Google Pay

Easily find past purchases from weekend getaways, past payments, and tickets you saved in your wallet. And if you choose, you can link your bank account, Gmail, and Google Photos to search even more transactions.



See <https://pay.google.com/about/>.

- Secure microcontroller
 - Arm® SecurCore® SC300™ 32-bit RISC core cadenced at 100 MHz
 - Up to 2048 Kbytes of user Flash memory
 - 2 Kbytes of memory cache
 - 64 Kbytes of user RAM
 - Power saving Standby and Hibernate states

See <https://www.st.com/en/secure-mcus/st54j.html>.

20. Google also knowingly and intentionally induces infringement of one or more claims of the '706 Patent in violation of 35 U.S.C. § 271(b). As of at least the filing and service of this complaint, Google has knowledge of the '706 Patent and the infringing nature of the Accused Products. Despite this knowledge of the '706 Patent, Google continues to actively encourage and instruct its customers and end users (for example, through user manuals and online instruction materials on its website, and other online publications cited above) to use the Accused Products in ways that directly infringe the '706 Patent, for example by utilizing the NFC functionality on the Accused Products and/or mobile payment applications, such as Google Pay, in an infringing manner. Google does so knowing and intending (or with willful blindness to the fact) that its customers and end users will commit these infringing acts. Google also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the '706 Patent, thereby specifically intending for and inducing its customers to infringe the '706 Patent through the customers' normal and customary use of the Accused Products.

21. Google has also infringed, and continues to infringe, one or more claims of the '706 Patent by selling, offering for sale, or importing into the United States, the Accused Products, knowing that the Accused Products constitute a material part of the inventions claimed in the '706 Patent, are especially made or adapted to infringe the '706 Patent, and are not staple articles or

commodities of commerce suitable for non-infringing use. Google has been, and currently is, contributorily infringing the '706 Patent in violation of 35 U.S.C. §§ 271(c) and/or (f).

22. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, Google has injured Plaintiff and is liable for infringement of the '706 Patent pursuant to 35 U.S.C. § 271.

23. As a result of Google's infringement of the '706 Patent, Plaintiff is entitled to monetary damages (past, present, and future) in an amount adequate to compensate for Google's infringement, but in no event less than a reasonable royalty for the use made of the invention by Google, together with interest and costs as fixed by the Court.

COUNT II

INFRINGEMENT OF U.S. PATENT NO. 8,816,827

24. Plaintiff realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

25. Google has been and is now directly infringing the '827 Patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a), including by making, using, selling, and/or offering for sale in the United States or importing into the United States infringing products, including at least the Accused Products identified above. The Accused Products satisfy all of the claim limitations of one or more claims of the '827 Patent, including but not limited to claim 22.

26. Claim 22 of the '827 Patent recites a "contactlessly communicating portable data carrier." To the extent the preamble is limiting, the Accused Products include portable data carriers that are capable of contactless communication through the use of Near Field Communication (NFC) technology. For example, Google advertises that the Accused Products support NFC:

Google Pixel 5a with 5G

Overview

Tech Specs

Compare

Trade-in & Financing

Setup & Tips

Wireless and Location

Wi-Fi 2.4 GHz + 5 GHz 802.11a/b/g/n/ac 2x2 MIMO

Bluetooth® v5.0 + LE, A2DP (HD codecs: AptX, AptX HD, LDAC, AAC)

NFC

Google Cast

See https://store.google.com/us/product/pixel_5a_5g_specs?hl=en-US.

27. Claim 22 of the '827 Patent recites that the portable data carrier comprises “at least a first and second application stored thereon.” The Accused Products are configured to store at least two applications. For example, the Accused Products are configured to store at least two applications that utilize NFC:

Service selection

When the user taps a device to an NFC reader, the Android system needs to know which HCE service the NFC reader wants to communicate with. The ISO/IEC 7816-4 specification defines a way to select applications, centered around an Application ID (AID). An AID consists of up to 16 bytes. If you are emulating cards for an existing NFC reader infrastructure, the AIDs that those readers look for are typically well-known and publicly registered (for example, the AIDs of payment networks such as Visa and MasterCard).

If you want to deploy new reader infrastructure for your own application, you must register your own AIDs. The registration procedure for AIDs is defined in the ISO/IEC 7816-5 specification. We recommend registering an AID as per 7816-5 if you are deploying a HCE application for Android, because it avoids collisions with other applications.

AID conflict resolution

Multiple `HostApuService` components may be installed on a single device, and the same AID can be registered by more than one service. Android resolves AID conflicts differently depending on which category an AID belongs to. Each category may have a different conflict resolution policy.

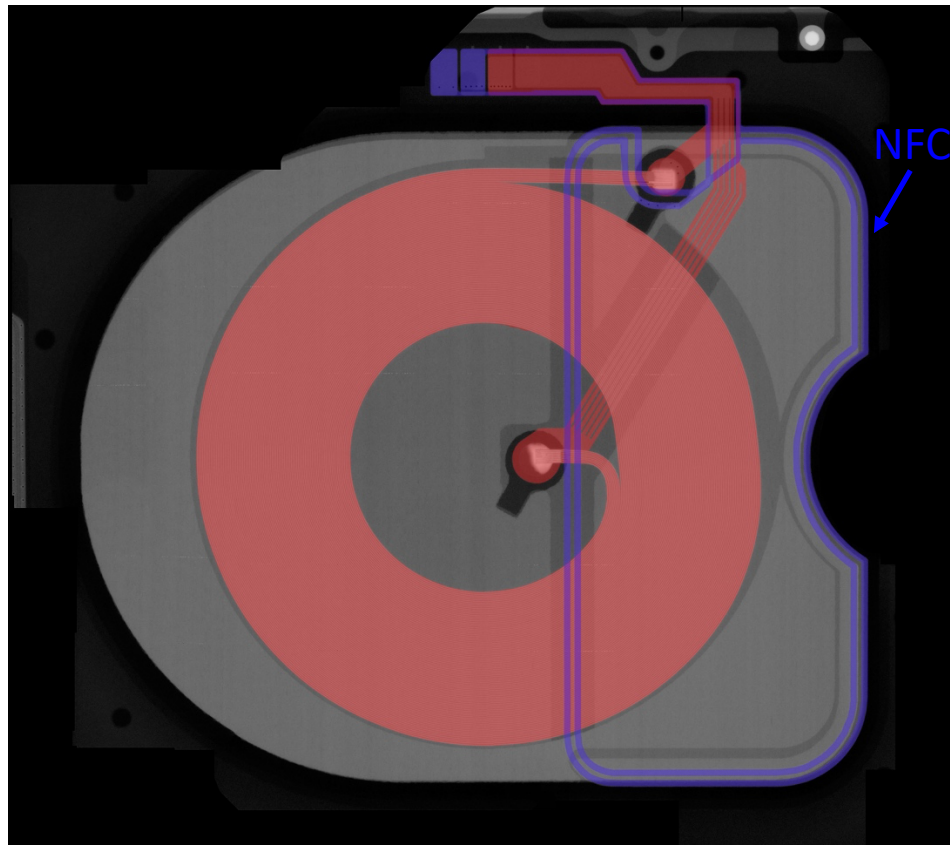
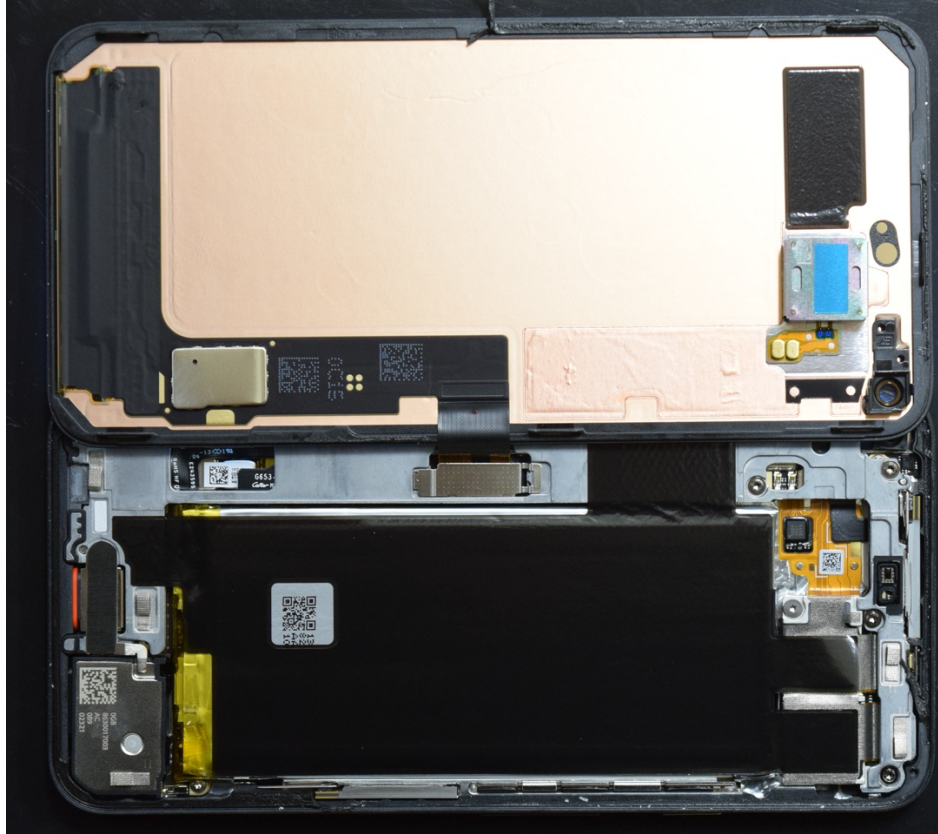
For some categories, such as payment, the user might be able to select a default service in the Android settings UI. For other categories, the policy might be to always ask the user which service to invoke in case of conflict. For information about how to query the conflict resolution policy for a certain category, see `getSelectionModeForCategory()`.

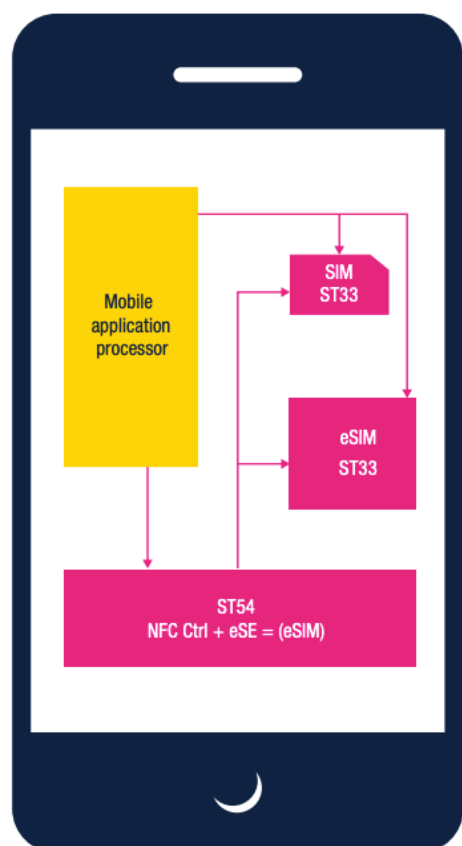
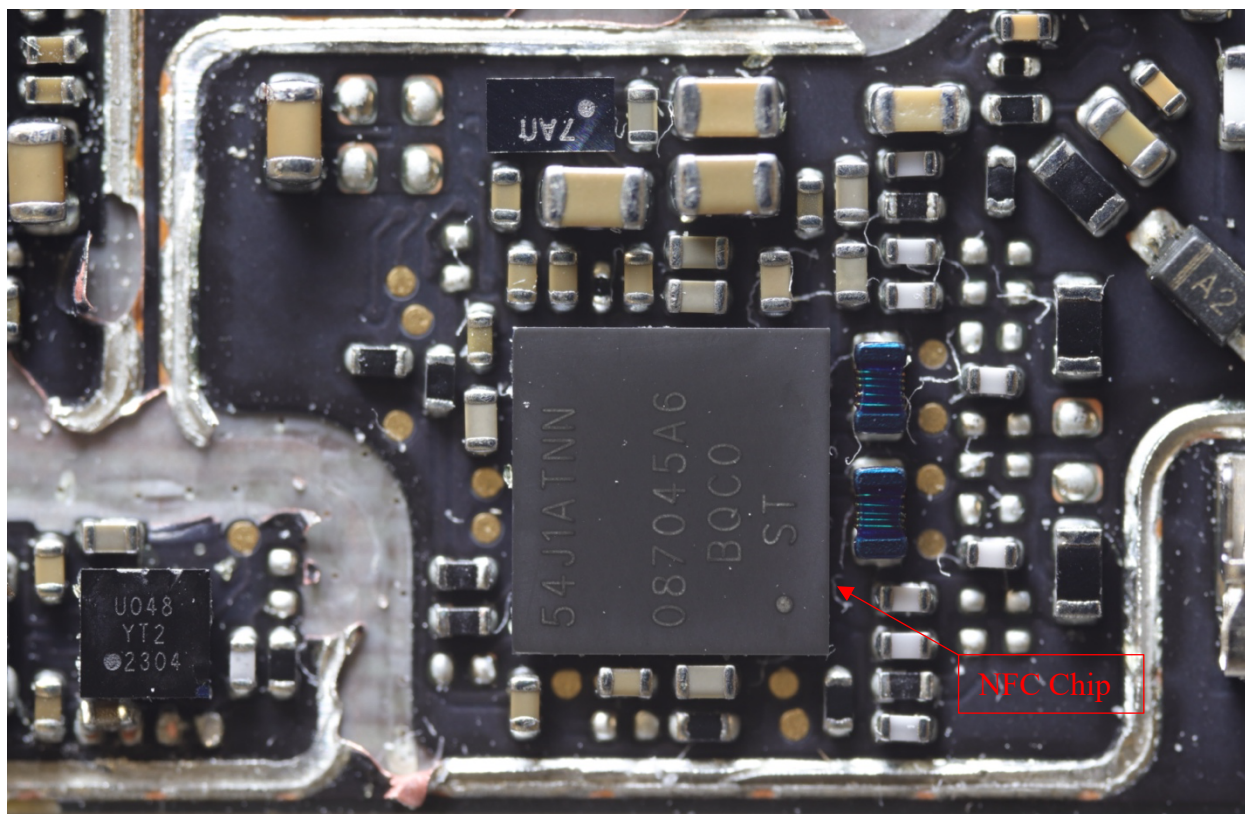
The following is an example of the corresponding `apduservice.xml` file registering two AIDs:

```
<offhost-apdu-service xmlns:android="http://schemas.android.com/apk/res/android"
    android:description="@string/servicedesc">
  <aid-group android:description="@string/subscription" android:category="other">
    <aid-filter android:name="F0010203040506" />
    <aid-filter android:name="F0394148148100" />
  </aid-group>
</offhost-apdu-service>
```

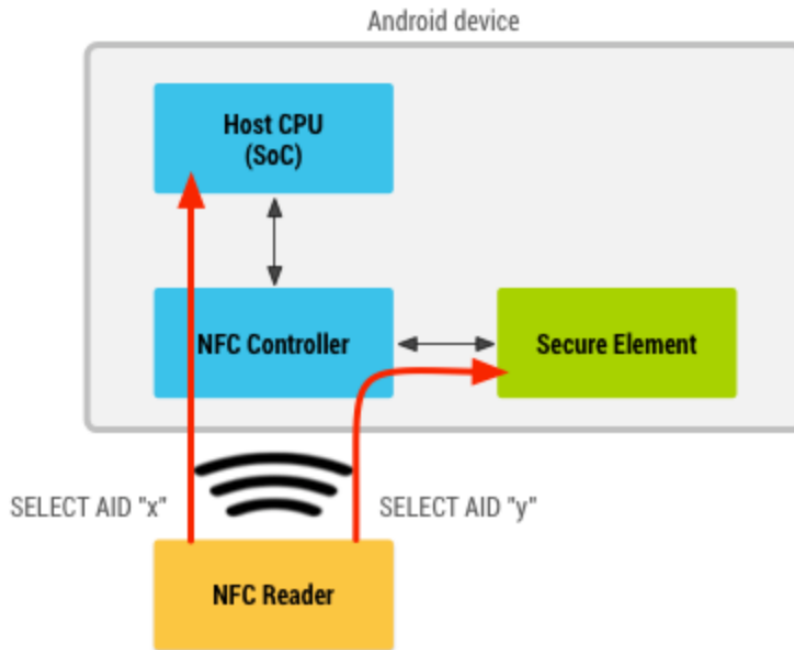
See <https://developer.android.com/guide/topics/connectivity/nfc/hce>.

28. Claim 22 of the '827 Patent recites “a communication device for controlling communication between a reading device and the at least first and second applications.” The Accused Products contain a communication device configured to control communication between a reading device and the at least first and second applications. For example, the Accused Products utilize an NFC antenna, NFC chip, and related hardware and software to control communication with a reading device and at least a first and second application, as shown in the exemplary Google Pixel 5:





See <https://www.st.com/en/secure-mcus/st54j.html>; see also https://www.emvco.com/wp-content/uploads/approved_products/uploaded/loa/MTA_LOA_GOLL_02519_20Oct20_SHORT.pdf.



See <https://developer.android.com/guide/topics/connectivity/nfc/hce>.

29. Claim 22 recites “wherein the communication device is configured to generate a first communication-readiness signal to the reading device which indicates to the reading device a communication readiness for the first application and a second communication-readiness signal to the reading device which indicates the reading device a communication readiness for the second application and comprise an identification number assigned to the corresponding communication-readiness application.” The Accused Products contain a communication device that is configured to generate a first communication-readiness signal to the reading device which indicates to the reading device a communication readiness for the first application and a second communication-readiness signal to the reading device which indicates the reading device a communication readiness for the second application and comprise an identification number assigned to the

corresponding communication-readiness application. For example, the communication device generates communication-readiness signals to an NFC reader which comprise of an Application ID (AID) that corresponds to an application:

Service selection

When the user taps a device to an NFC reader, the Android system needs to know which HCE service the NFC reader wants to communicate with. The ISO/IEC 7816-4 specification defines a way to select applications, centered around an Application ID (AID). An AID consists of up to 16 bytes. If you are emulating cards for an existing NFC reader infrastructure, the AIDs that those readers look for are typically well-known and publicly registered (for example, the AIDs of payment networks such as Visa and MasterCard).

If you want to deploy new reader infrastructure for your own application, you must register your own AIDs. The registration procedure for AIDs is defined in the ISO/IEC 7816-5 specification. We recommend registering an AID as per 7816-5 if you are deploying a HCE application for Android, because it avoids collisions with other applications.

AID conflict resolution

Multiple `HostApuService` components may be installed on a single device, and the same AID can be registered by more than one service. Android resolves AID conflicts differently depending on which category an AID belongs to. Each category may have a different conflict resolution policy.

For some categories, such as payment, the user might be able to select a default service in the Android settings UI. For other categories, the policy might be to always ask the user which service to invoke in case of conflict. For information about how to query the conflict resolution policy for a certain category, see `getSelectionModeForCategory()`.

The following is an example of the corresponding `apdu-service.xml` file registering two AIDs:

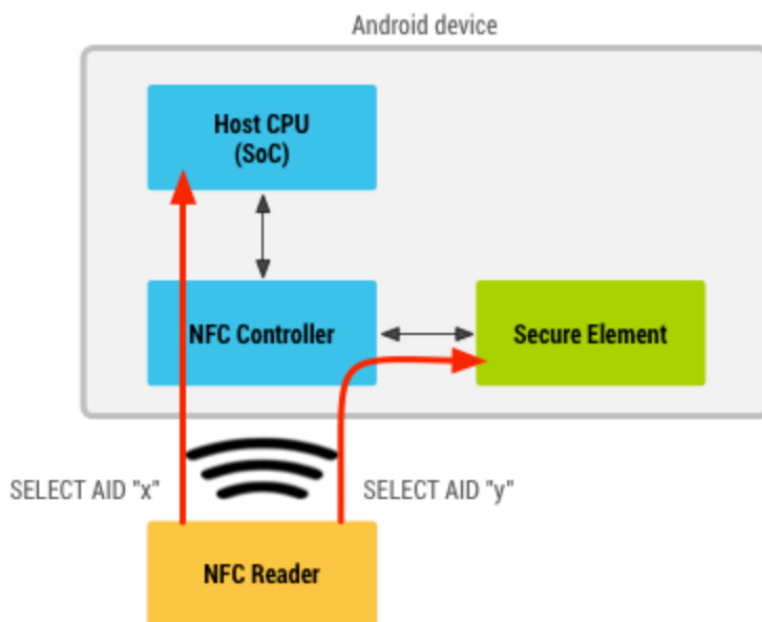
```
<offhost-apdu-service xmlns:android="http://schemas.android.com/apk/res/android"
    android:description="@string/servicedesc">
  <aid-group android:description="@string/subscription" android:category="other">
    <aid-filter android:name="F0010203040506"/>
    <aid-filter android:name="F0394148148100"/>
  </aid-group>
</offhost-apdu-service>
```

Nfc-A (ISO/IEC 14443 type A) protocol anti-collision and activation

As part of the Nfc-A protocol activation, multiple frames are exchanged.

In the first part of the exchange, the HCE device presents its UID; HCE devices should be assumed to have a random UID. This means that on every tap, the UID that is presented to the reader is a randomly generated UID. Because of this, NFC readers should not depend on the UID of HCE devices as a form of authentication or identification.

The NFC reader can subsequently select the HCE device by sending a `SEL_REQ` command. The `SEL_RES` response of the HCE device has at least the 6th bit (0x20) set, indicating that the device supports ISO-DEP. Note that other bits in the `SEL_RES` may be set as well, indicating for example support for the NFC-DEP (p2p) protocol. Since other bits may be set, readers wanting to interact with HCE devices should explicitly check for the 6th bit only, and **not** compare the complete `SEL_RES` with a value of 0x20.



See <https://developer.android.com/guide/topics/connectivity/nfc/hce>.

30. Claim 22 of the '827 Patent recites “wherein the first communication-readiness signal is generated for a first group of applications comprising a first plurality of applications including the first application, and the first identification number is assigned to every application in the first group, and the second communication-readiness signal is generated for a second group of applications comprising a second plurality of applications including the second application, and the second identification number is assigned to every application in the second group, the first communication-readiness signal indicating to the reading device the communication readiness of

every application of the first group, and the second communication-readiness signal indicating to the reading device the communication readiness of every application of the second group.” The Accused Products generate the first communication-readiness signal for a first group of applications comprising a first plurality of applications including the first application, and the first identification number is assigned to every application in the first group, and the second communication-readiness signal is generated for a second group of applications comprising a second plurality of applications including the second application, and the second identification number is assigned to every application in the second group, the first communication-readiness signal indicating to the reading device the communication readiness of every application of the first group, and the second communication-readiness signal indicating to the reading device the communication readiness of every application of the second group. For example, the Accused Products are configured to generate Application IDs (AID) for at least a first and second group of applications:

AID groups

In some cases, an HCE service may need to register multiple AIDs and be set as the default handler for all of the AIDs in order to implement a certain application. Some AIDs in the group going to another service isn't supported.

A list of AIDs that are kept together is called an AID group. For all AIDs in an AID group, Android guarantees one of the following:

- All AIDs in the group are routed to this HCE service.
- No AIDs in the group are routed to this HCE service (for example, because the user preferred another service which requested one or more AIDs in your group as well).

In other words, there is no in-between state, where some AIDs in the group can be routed to one HCE service, and some to another.

AID groups and categories

You can associate each AID group with a category. This allows Android to group HCE services together by category, and that in turn allows the user to set defaults at the category level instead of the AID level. Avoid mentioning AIDs in any user-facing parts of your application, because they don't mean anything to the average user.

Android 4.4 and higher supports two categories:

- `CATEGORY_PAYMENT` (covering industry-standard payment apps)
- `CATEGORY_OTHER` (for all other HCE apps)

Nfc-A (ISO/IEC 14443 type A) protocol anti-collision and activation

As part of the Nfc-A protocol activation, multiple frames are exchanged.

In the first part of the exchange, the HCE device presents its UID; HCE devices should be assumed to have a random UID. This means that on every tap, the UID that is presented to the reader is a randomly generated UID. Because of this, NFC readers should not depend on the UID of HCE devices as a form of authentication or identification.

The NFC reader can subsequently select the HCE device by sending a `SEL_REQ` command. The `SEL_RES` response of the HCE device has at least the 6th bit (0x20) set, indicating that the device supports ISO-DEP. Note that other bits in the `SEL_RES` may be set as well, indicating for example support for the NFC-DEP (p2p) protocol. Since other bits may be set, readers wanting to interact with HCE devices should explicitly check for the 6th bit only, and **not** compare the complete `SEL_RES` with a value of 0x20.

See <https://developer.android.com/guide/topics/connectivity/nfc/hce>.

31. Google also knowingly and intentionally induces infringement of one or more claims of the '827 Patent in violation of 35 U.S.C. § 271(b). As of at least the filing and service of this complaint, Google has knowledge of the '827 Patent and the infringing nature of the Accused Products. Despite this knowledge of the '827 Patent, Google continues to actively encourage and instruct its customers and end users (for example, through user manuals and online instruction materials on its website, and other online publications cited above) to use the Accused Products in ways that directly infringe the '827 Patent, for example by utilizing the NFC functionality on the Accused Products and/or mobile payment applications, such as Google Pay, in an infringing manner. Google does so knowing and intending (or with willful blindness to the fact) that its customers and end users will commit these infringing acts. Google also continues to

make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the '827 Patent, thereby specifically intending for and inducing its customers to infringe the '827 Patent through the customers' normal and customary use of the Accused Products.

32. Google has also infringed, and continues to infringe, one or more claims of the '827 Patent by selling, offering for sale, or importing into the United States, the Accused Products, knowing that the Accused Products constitute a material part of the inventions claimed in the '827 Patent, are especially made or adapted to infringe the '827 Patent, and are not staple articles or commodities of commerce suitable for non-infringing use. Google has been, and currently is, contributorily infringing the '827 Patent in violation of 35 U.S.C. §§ 271(c) and/or (f).

33. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, Google has injured Plaintiff and is liable for infringement of the '827 Patent pursuant to 35 U.S.C. § 271.

34. As a result of Google's infringement of the '827 Patent, Plaintiff is entitled to monetary damages (past, present, and future) in an amount adequate to compensate for Google's infringement, but in no event less than a reasonable royalty for the use made of the invention by Google, together with interest and costs as fixed by the Court.

COUNT III

INFRINGEMENT OF U.S. PATENT NO. 8,205,249

35. Plaintiff realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

36. Google has been and is now directly infringing the '249 Patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271(a), including by making, using, selling, and/or offering for sale in the United States or importing into the United States infringing

products, including at least the Accused Products identified above. The Accused Products satisfy all of the claim limitations of one or more claims of the '249 Patent, including but not limited to claim 10.

37. Claim 10 recites a “portable data carrier for performing a security-operation within a secure electronic transaction.” To the extent the preamble is limiting, the Accused Products include a portable data carrier for performing a security-operation within a secure electronic transaction. For example, the Accused Products support mobile payment applications, such as Google Pay, which enable a security-operation within a secure electronic transaction:

Make contactless payments with your Pixel phone

You can use tap and pay for purchases at retailers that accept contactless payments.

See <https://support.google.com/pixelphone/answer/3470787?hl=en>.

What is Google Pay?

Google Pay brings together all the ways you can pay with Google.

Enter your card information once and use it to:

- Tap and pay to make purchases with your phone ([See country and device availability](#)).
- Buy items in apps and on websites ([See country availability](#)).
- Fill in forms automatically on Chrome ([Learn more](#)).
- Buy Google products.
- Send money to friends and family (US only).

See https://support.google.com/pay/answer/9026749?hl=en&ref_topic=7625138.

Only you can pay with your phone

Google Pay requires authentication – via a pin, pattern or biometric – to open the app or pay a person*. That means no one but you can make payments or see your information if your phone goes missing.


*Unlock requirements vary by country.

See <https://safety.google/pay/>.

38. Claim 10 of the '249 Patent recites that the portable data carrier is “arranged to perform different quality user authentication methods.” To the extent the preamble is limiting, the Accused Products include a portable data carrier that is arranged to perform different quality user authentication methods. For example, the Accused Products support mobile payment applications, such as Google Pay, which utilize different quality user authentication methods:

Add a debit or credit card



1. Open the Google Pay app  .
 - If you have multiple accounts in Google Pay, you can select the account to change:
 - a. In the Google Pay app, at the top right, tap your profile picture or initial.
 - b. Tap the account you want to use to add a debit or credit card.
2. Swipe up from the bottom.
3. Tap **Add a card** > **Debit or credit card**.
4. Use the camera to capture your card info or enter it manually.
5. If you're asked to verify your payment method, choose an option from the list. [Learn how to verify your payment method](#).
6. Find and enter the verification code.

After you add a card, you might find a small charge on your account from Google Pay. This charge checks that your card and account are valid. The charge disappears and doesn't affect your balance.

<https://support.google.com/pay/answer/7625139?hl=en&co=GENIE.Platform%3DAndroid&oco=1#zippy=%2Cadd-a-debit-or-credit-card>.

Only you can pay with your phone

Google Pay requires authentication – via a pin, pattern or biometric – to open the app or pay a person*. That means no one but you can make payments or see your information if your phone goes missing.

*Unlock requirements vary by country.

See <https://safety.google/pay/>.

Set up screen lock to make contactless payments

To make contactless payments with Google Pay, you need to set up a screen lock on your device for your security.

[Android](#) iPhone & iPad

Important: Screen lock is optional for e-money, QUICPay, and iD users in Japan.

You can unlock Google Pay with the following methods:

- PIN
- Pattern
- Password
- Fingerprint
- Iris scan
- 3D face unlock

No unlock needed for smaller payments

To make contactless payments, you need to unlock your phone. You won't need to unlock it for certain small payments.

United States	Unlock is required for all transactions except for transit.
---------------	---

See <https://support.google.com/pay/answer/7644132?co=GENIE.Platform=Android&hl=en>.

Skip device unlock

As users walk through turnstiles or board buses, it's important for them to be able to pay for their transit with their phones and complete transactions easily.

Google Pay allows users to pay on transit terminals without the need to unlock their device. To pay, the user taps the power button to light the screen, then holds their phone to the reader. The device can remain locked, and displays a tick on the screen when the transaction is successful.

See <https://developers.google.com/pay/transit/open-loop/mobile-features/skip-device-unlock>.

39. Claim 10 recites “wherein the difference in quality of said user authentication methods varies between an inherently relatively lower quality and an inherently relatively higher quality from a security perspective.” To the extent the preamble is limiting, the Accused Products include a data carrier arranged to perform different quality user authentication methods, wherein the difference in quality of said user authentication methods varies between an inherently relatively lower quality and an inherently relatively higher quality from a security perspective. For example, the Accused Products support mobile payment applications, such as Google Pay, which utilize different authentication methods that vary in quality from a security perspective:

Only you can pay with your phone

Google Pay requires authentication – via a pin, pattern or biometric – to open the app or pay a person*. That means no one but you can make payments or see your information if your phone goes missing.

*Unlock requirements vary by country.

See <https://safety.google/pay/>.

Set up screen lock to make contactless payments

To make contactless payments with Google Pay, you need to set up a screen lock on your device for your security.

[Android](#) iPhone & iPad

Important: Screen lock is optional for e-money, QUICPay, and iD users in Japan.

You can unlock Google Pay with the following methods:

- PIN
- Pattern
- Password
- Fingerprint
- Iris scan
- 3D face unlock

No unlock needed for smaller payments

To make contactless payments, you need to unlock your phone. You won't need to unlock it for certain small payments.

United States	Unlock is required for all transactions except for transit.
---------------	---

See <https://support.google.com/pay/answer/7644132?co=GENIE.Platform=Android&hl=en>.

Skip device unlock

As users walk through turnstiles or board buses, it's important for them to be able to pay for their transit with their phones and complete transactions easily.

Google Pay allows users to pay on transit terminals without the need to unlock their device. To pay, the user taps the power button to light the screen, then holds their phone to the reader. The device can remain locked, and displays a tick on the screen when the transaction is successful.

See <https://developers.google.com/pay/transit/open-loop/mobile-features/skip-device-unlock>.

40. Claim 10 of the '249 Patent recites that “the portable data carrier is arranged to perform a user authentication using one of said implemented user authentication methods.” The Accused Products include a portable data carrier arranged to perform a user authentication using one of said implemented user authentication methods. For example, the Accused Products support mobile payment applications, such as Google Pay, which utilize different user authentication methods:

Only you can pay with your phone

Google Pay requires authentication – via a pin, pattern or biometric – to open the app or pay a person*. That means no one but you can make payments or see your information if your phone goes missing.

*Unlock requirements vary by country.

See <https://safety.google/pay/>.

Set up screen lock to make contactless payments

To make contactless payments with Google Pay, you need to set up a screen lock on your device for your security.

[Android](#) iPhone & iPad

Important: Screen lock is optional for e-money, QUICPay, and iD users in Japan.

You can unlock Google Pay with the following methods:

- PIN
- Pattern
- Password
- Fingerprint
- Iris scan
- 3D face unlock

No unlock needed for smaller payments

To make contactless payments, you need to unlock your phone. You won't need to unlock it for certain small payments.

United States	Unlock is required for all transactions except for transit.
---------------	---

See <https://support.google.com/pay/answer/7644132?co=GENIE.Platform=Android&hl=en>.

Skip device unlock

As users walk through turnstiles or board buses, it's important for them to be able to pay for their transit with their phones and complete transactions easily.

Google Pay allows users to pay on transit terminals without the need to unlock their device. To pay, the user taps the power button to light the screen, then holds their phone to the reader. The device can remain locked, and displays a tick on the screen when the transaction is successful.

See <https://developers.google.com/pay/transit/open-loop/mobile-features/skip-device-unlock>.

41. Claim 10 of the '249 Patent recites that “the portable data carrier is arranged to confirm the authentication to a terminal.” The Accused Products include a portable data carrier arranged to confirm the authentication to a terminal. For example, the Accused Products support mobile payment applications, such as Google Pay, and confirm the authentication to a terminal:

Pay in a store

Step 1: Wake up & unlock your phone

Turn on your phone screen, and then unlock your phone. You do not need to open the Google Pay app.

Step 2: Hold the back of your phone close to the payment reader for a few seconds

When you're done paying, a blue check mark will appear on the screen.

See <https://support.google.com/pay/answer/7644134?hl=en&co=GENIE.Platform%3DAndroid>.

2. To make a purchase, a customer taps their mobile device on a point-of-sale terminal or chooses to pay in your mobile app. Google Pay responds with the customer's tokenized card and a cryptogram which acts as a one-time-use password. The card network validates the cryptogram and matches the token with the customer's actual card number.

See <https://support.google.com/pay/merchants/answer/6345242?hl=en#zippy=%2Cdetailed-google-pay-transaction-process-in-stores>.

42. Claim 10 of the '249 Patent recites “wherein the data carrier is arranged to create quality information about said user authentication method used and to attach such quality information to the result of the security establishing operation.” The Accused Products include a portable data carrier that is arranged to create quality information about the user authentication method used and to attach such quality information to the result of the security establishing operation. For example, on information and belief, the Accused Products include a data carrier that creates quality information about the type of authentication method used by a user and attaches that information to the result of the security establishing operation in an electronic transaction.

43. Google also knowingly and intentionally induces infringement of one or more claims of the '249 Patent in violation of 35 U.S.C. § 271(b). As of at least the filing and service of this complaint, Google has knowledge of the '249 Patent and the infringing nature of the Accused Products. Despite this knowledge of the '249 Patent, Google continues to actively encourage and instruct its customers and end users (for example, through user manuals and online instruction materials on its website, and other online publications cited above) to use the Accused Products in ways that directly infringe the '249 Patent, for example by utilizing the NFC functionality on the Accused Products and/or mobile payment applications, such as Google Pay, in an infringing manner. Google does so knowing and intending (or with willful blindness to the fact) that its customers and end users will commit these infringing acts. Google also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the '249 Patent, thereby specifically intending for and inducing its customers to infringe the '249 Patent through the customers' normal and customary use of the Accused Products.

44. Google has also infringed, and continues to infringe, one or more claims of the '249 Patent by selling, offering for sale, or importing into the United States, the Accused Products, knowing that the Accused Products constitute a material part of the inventions claimed in the '249 Patent, are especially made or adapted to infringe the '249 Patent, and are not staple articles or commodities of commerce suitable for non-infringing use. Google has been, and currently is, contributorily infringing the '249 Patent in violation of 35 U.S.C. §§ 271(c) and/or (f).

45. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, Google has injured Plaintiff and is liable for infringement of the '249 Patent pursuant to 35 U.S.C. § 271.

46. As a result of Google's infringement of the '249 Patent, Plaintiff is entitled to monetary damages (past, present, and future) in an amount adequate to compensate for Google's infringement, but in no event less than a reasonable royalty for the use made of the invention by Google, together with interest and costs as fixed by the Court.

COUNT IV

INFRINGEMENT OF U.S. PATENT NO. 8,174,360

47. Plaintiff realleges and incorporates by reference the foregoing paragraphs as if fully set forth herein.

48. Google has been and is now directly infringing the '360 Patent, literally and/or under the doctrine of equivalents, in violation of 35 U.S.C. § 271, including by making, using, selling, and/or offering for sale in the United States or importing into the United States infringing products, including at least the Accused Products identified above. The Accused Products satisfy all of the claim limitations of one or more claims of the '360 Patent, including but not limited to claim 1.

49. Claim 1 of the '360 Patent recites a "communication apparatus for setting up a data connection between intelligent devices." To the extent the preamble is limiting, the Accused Products include a communication apparatus for setting up a data connection between intelligent devices. For example, Google advertises that the Accused Products support NFC:

Google Pixel 5a with 5G

Overview

Tech Specs

Compare

Trade-in & Financing

Setup & Tips

Wireless and Location

Wi-Fi 2.4 GHz + 5 GHz 802.11a/b/g/n/ac 2x2 MIMO

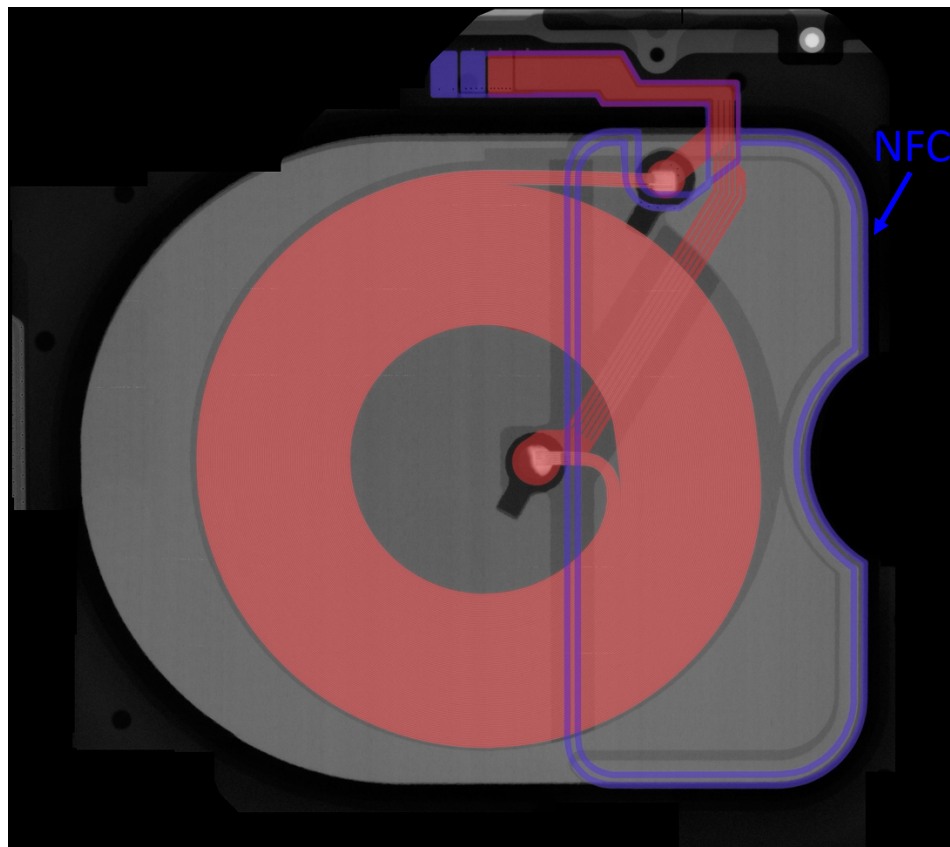
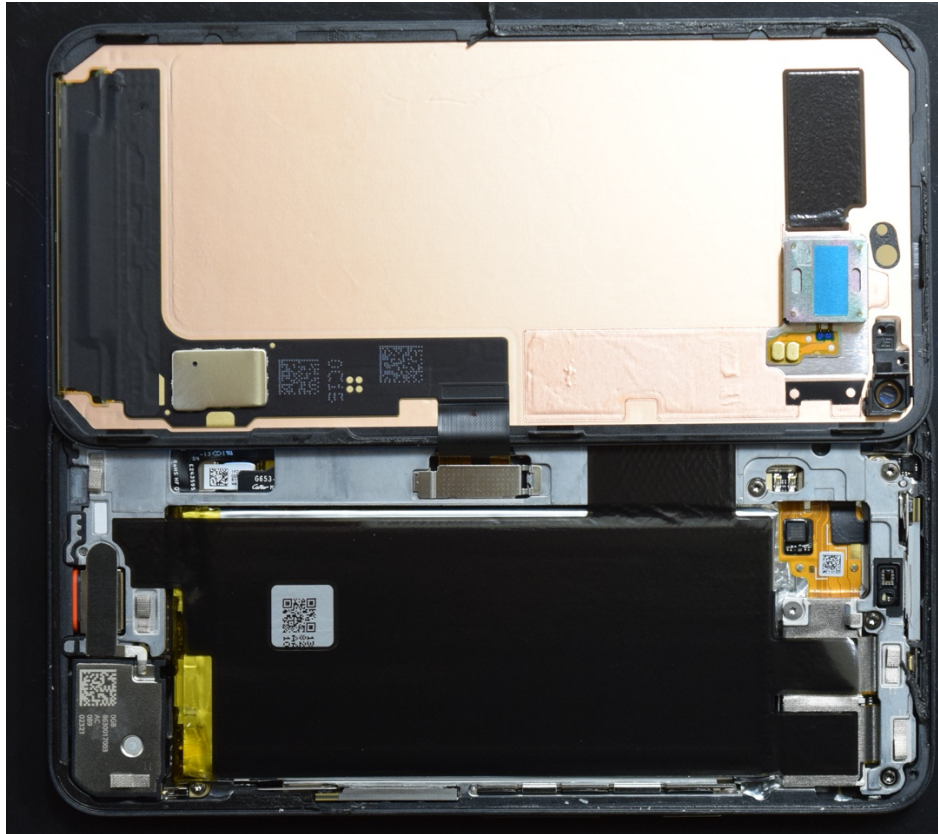
Bluetooth® v5.0 + LE, A2DP (HD codecs: AptX, AptX HD, LDAC, AAC)

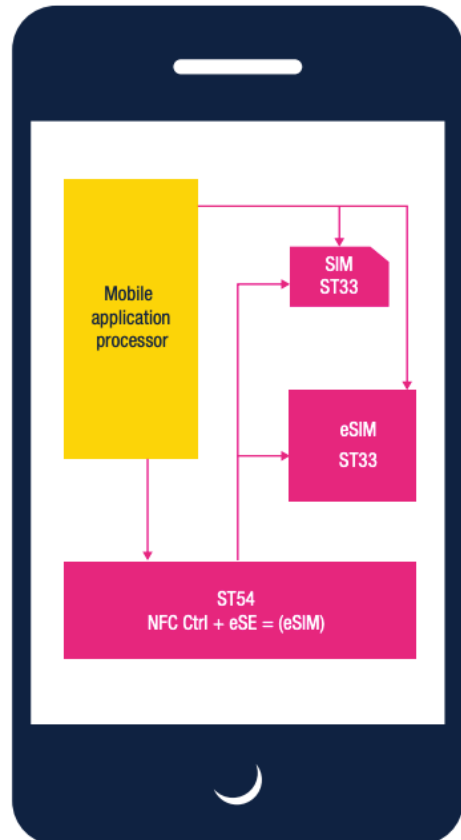
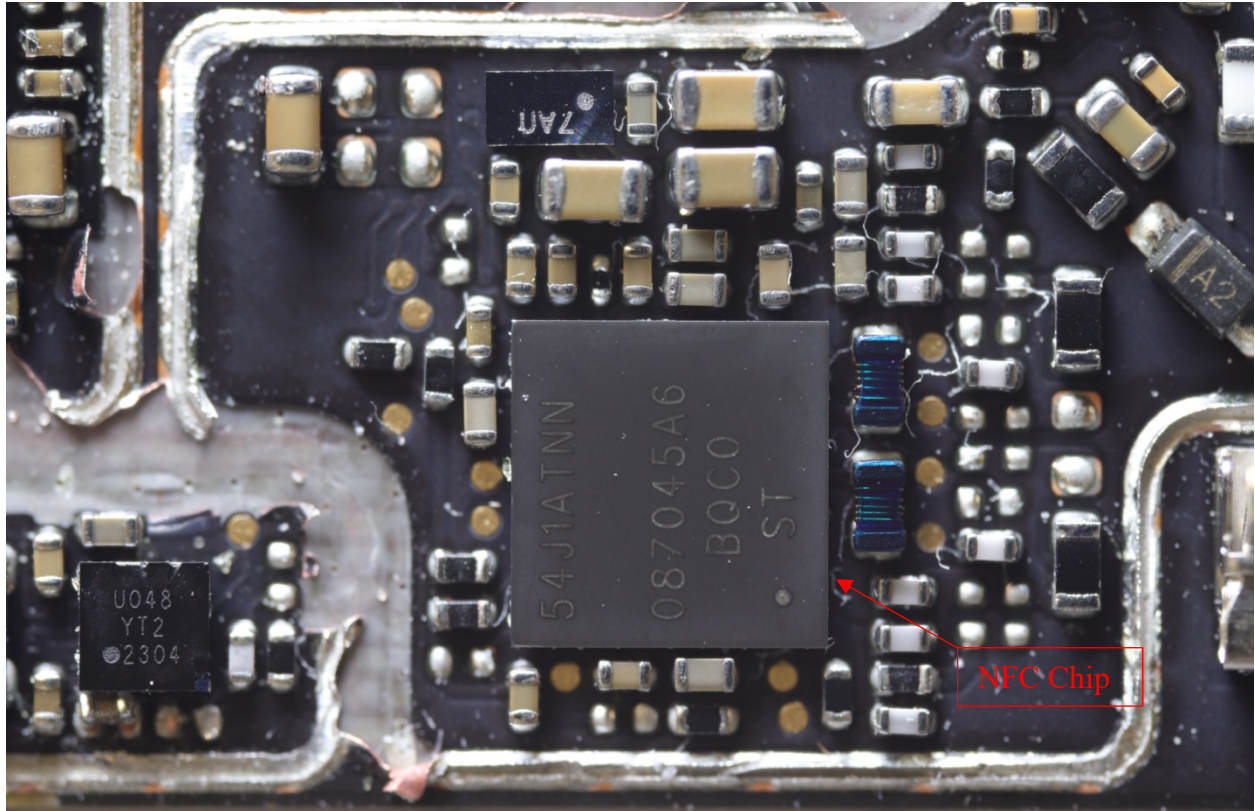
NFC

Google Cast

See https://store.google.com/us/product/pixel_5a_5g_specs?hl=en-US.

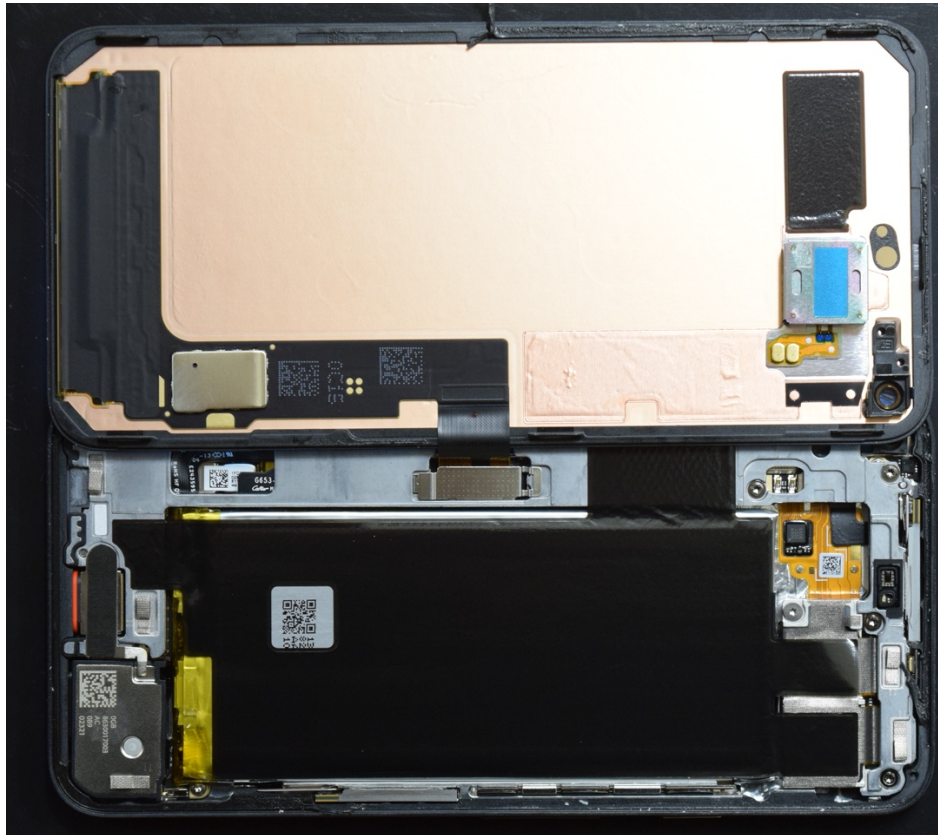
50. Claim 1 of the '360 Patent recites an “apparatus” comprising “a transmission oscillator for carrying out a contactless data exchange, said oscillator including a coil.” The Accused Products include a transmission oscillator for carrying out a contactless data exchange, said oscillator including a coil. For example, the Accused Products include an NFC antenna, NFC chip, and related hardware and software, as shown in the exemplary Google Pixel 5:

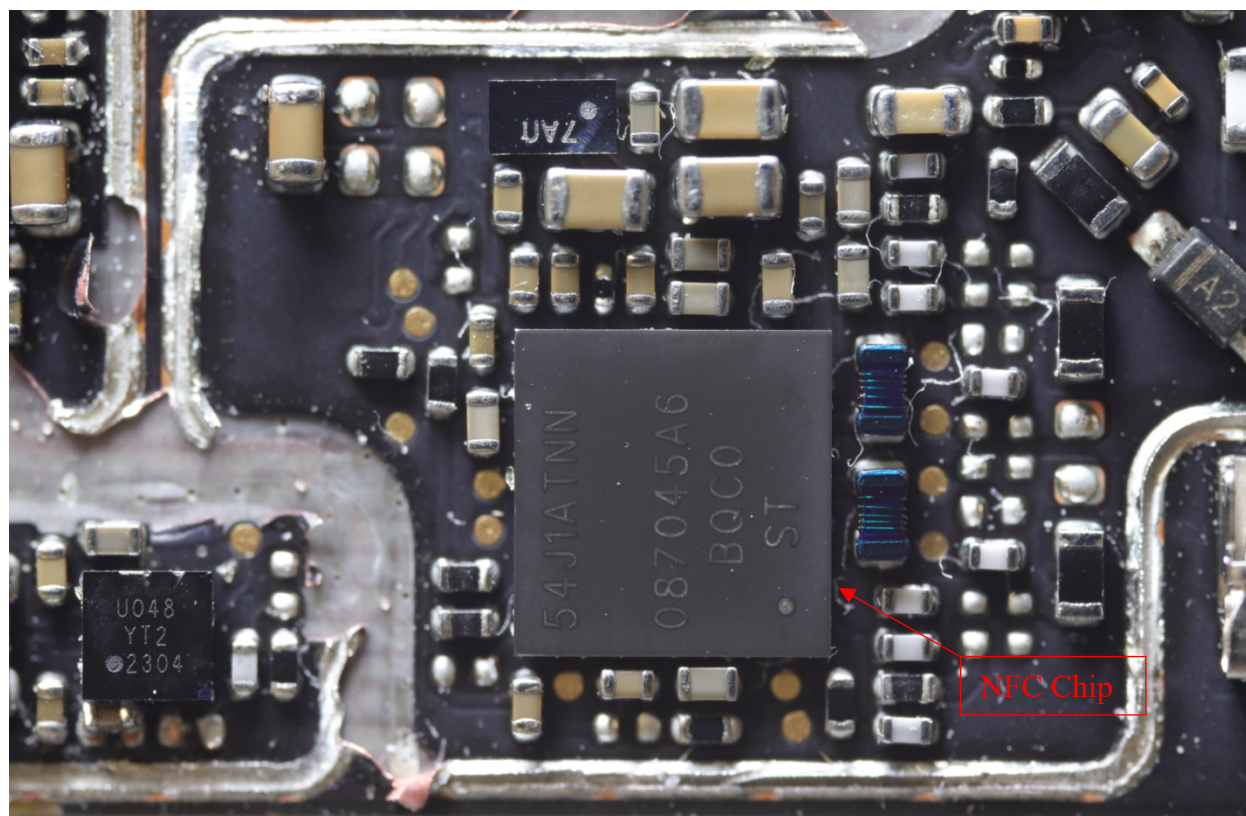
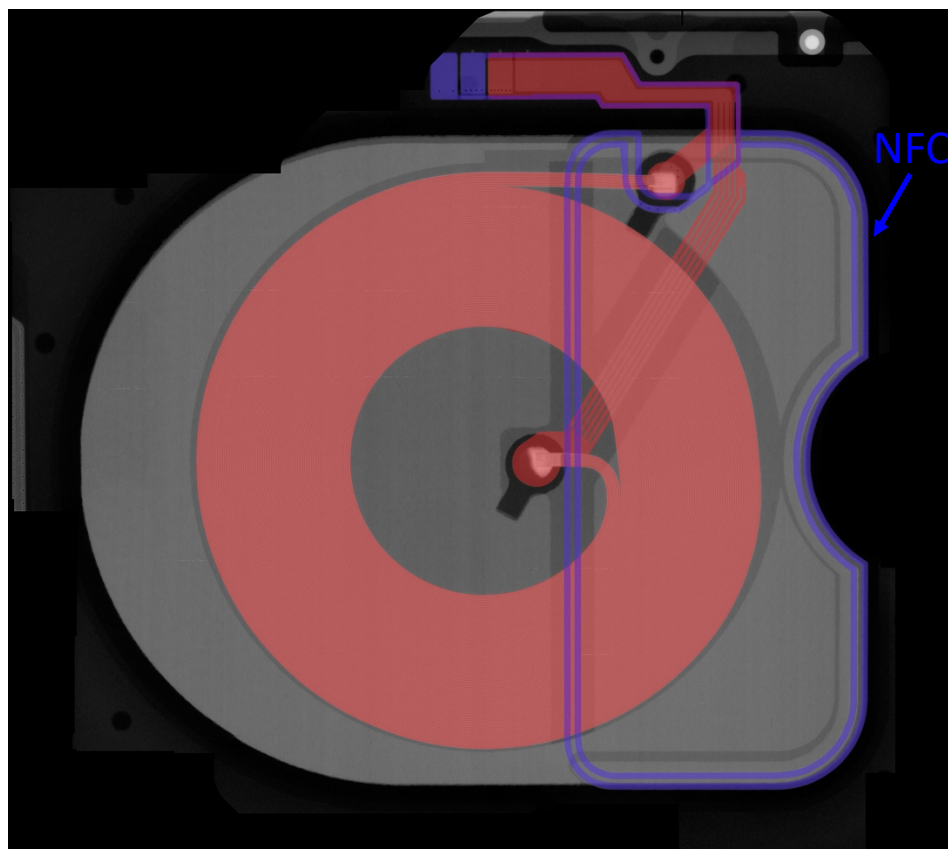


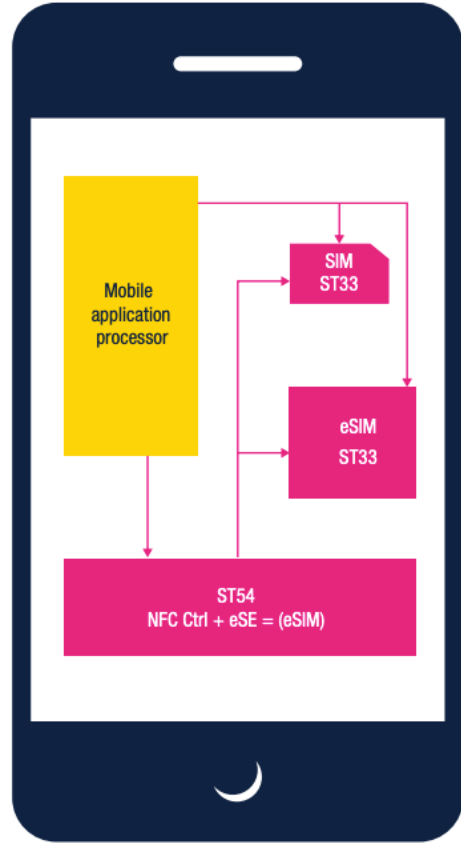


See <https://www.st.com/en/secure-mcus/st54j.html>; see also https://www.emvco.com/wp-content/uploads/approved_products/uploaded/loa/MTA_LOA_GOLL_02519_20Oct20_SHORT.pdf.

51. Claim 1 of the '360 Patent recites an “apparatus” comprising “a communication element which is connected to the coil and to a data processing component of an intelligent device and which emits search signals via the coil to receive a response from another intelligent device.” The Accused Products include a communication element which is connected to the coil and to a data processing component of an intelligent device and which emits search signals via the coil to receive a response from another intelligent device. For example, teardowns show that the Accused Products include an NFC antenna, NFC chip, and related hardware and software, as shown in the exemplary Google Pixel 5:







See <https://www.st.com/en/secure-mcus/st54j.html>; see also https://www.emvco.com/wp-content/uploads/approved_products/uploaded/loa/MTA_LOA_GOLL_02519_20Oct20_SHORT.pdf.

52. Claim 1 of the '360 Patent recites an “apparatus” comprising “a measuring device for monitoring a property of the transmission oscillator which outputs a control signal when ascertaining a change of the monitored property, the monitored property of the transmission oscillator includes the frequency or impedance of the transmission oscillator in resonance.” The Accused Products include a measuring device for monitoring a property of the transmission oscillator which outputs a control signal when ascertaining a change of the monitored property, the monitored property of the transmission oscillator includes the frequency or impedance of the

transmission oscillator in resonance. For example, on information and belief, the Accused Products include low power modes for the NFC functionality that satisfy this limitation:

- NFC controller
 - Arm® Cortex®-M3 microcontroller
 - 100% re-flashing capability for firmware update
 - Enhanced active load modulation technology
 - Enhanced TX drive up to 2 W with support of an external 5 V DC/DC converter for TX supply
 - Optimized for extremely small or metal frame antennas
 - Optimized power consumption modes
 - Ultralow power Hibernate mode with selectable field detection for low-power mode support
 - Proprietary In-Frame Synchronization (IFS) in Card Emulation (CE) to ensure stability in battery Low and Switched OFF modes
 - System clock
 - Fractional-N PLL input range of 13.56 to 76.8 MHz
 - 27.12 MHz external crystal oscillator
 - Automatic wakeup via communication interfaces, internal timers, GPIO, RF field or tag detection

See https://www.st.com/en/secure-mcus/st54j.html#overview&secondary=st_all-features_sec-nav-tab/.

53. Claim 1 of the '360 Patent recites an “apparatus” comprising “a switching apparatus which is connected to the measuring device and the communication element and which switches on the communication element when it has received the control signal from the measuring device by connecting the communication element to an energy source.” The Accused Products include a switching apparatus which is connected to the measuring device and the communication element and which switches on the communication element when it has received the control signal from the measuring device by connecting the communication element to an energy source. For example, on information and belief, the Accused Products include low power modes for the NFC functionality that satisfy this limitation.

- NFC controller
 - Arm® Cortex®-M3 microcontroller
 - 100% re-flashing capability for firmware update
 - Enhanced active load modulation technology
 - Enhanced TX drive up to 2 W with support of an external 5 V DC/DC converter for TX supply
 - Optimized for extremely small or metal frame antennas
 - Optimized power consumption modes
 - Ultralow power Hibernate mode with selectable field detection for low-power mode support
 - Proprietary In-Frame Synchronization (IFS) in Card Emulation (CE) to ensure stability in battery Low and Switched OFF modes
 - System clock
 - Fractional-N PLL input range of 13.56 to 76.8 MHz
 - 27.12 MHz external crystal oscillator
 - Automatic wakeup via communication interfaces, internal timers, GPIO, RF field or tag detection

See https://www.st.com/en/secure-mcus/st54j.html#overview&secondary=st_all-features_sec-nav-tab/.

54. Google also knowingly and intentionally induces infringement of one or more claims of the '360 Patent in violation of 35 U.S.C. § 271(b). As of at least the filing and service of this complaint, Google has knowledge of the '360 Patent and the infringing nature of the Accused Products. Despite this knowledge of the '360 Patent, Google continues to actively encourage and instruct its customers and end users (for example, through user manuals and online instruction materials on its website, and other online publications cited above) to use the Accused Products in ways that directly infringe the '360 Patent, for example by utilizing the NFC functionality on the Accused Products, in an infringing manner. Google does so knowing and intending (or with willful blindness to the fact) that its customers and end users will commit these infringing acts. Google also continues to make, use, offer for sale, sell, and/or import the Accused Products, despite its knowledge of the '360 Patent, thereby specifically intending for and inducing its customers to infringe the '360 Patent through the customers' normal and customary use of the Accused Products.

55. Google has also infringed, and continues to infringe, one or more claims of the '360 Patent by selling, offering for sale, or importing into the United States, the Accused Products, knowing that the Accused Products constitute a material part of the inventions claimed in the '360 Patent, are especially made or adapted to infringe the '360 Patent, and are not staple articles or commodities of commerce suitable for non-infringing use. Google has been, and currently is, contributorily infringing the '360 Patent in violation of 35 U.S.C. §§ 271(c) and/or (f).

56. By making, using, offering for sale, selling and/or importing into the United States the Accused Products, Google has injured Plaintiff and is liable for infringement of the '360 Patent pursuant to 35 U.S.C. § 271.

57. As a result of Google's infringement of the '360 Patent, Plaintiff is entitled to monetary damages (past, present, and future) in an amount adequate to compensate for Google's infringement, but in no event less than a reasonable royalty for the use made of the invention by Google, together with interest and costs as fixed by the Court.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that this Court enter:

- a. A judgment in favor of Plaintiff that Google has infringed, either literally and/or under the doctrine of equivalents, the '706, '827, '249, and '360 Patents;
- b. A judgment and order requiring Google to pay Plaintiff its damages (past, present, and future), costs, expenses, and pre-judgment and post-judgment interest for Google's infringement of the '706, '827, '249, and '360 Patents;
- c. A judgment and order requiring Google to pay Plaintiff compulsory ongoing licensing fees, as determined by the Court in equity.
- d. A judgment and order requiring Google to provide an accounting and to pay

supplemental damages to Plaintiff, including without limitation, pre-judgment and post-judgment interest and compensation for infringing products released after the filing of this case that are not colorably different from the accused products;

e. A judgment and order finding that this is an exceptional case within the meaning of 35 U.S.C. § 285 and awarding to Plaintiff its reasonable attorneys' fees against Google; and

f. Any and all other relief as the Court may deem appropriate and just under the circumstances.

DEMAND FOR JURY TRIAL

Plaintiff, under Rule 38 of the Federal Rules of Civil Procedure, requests a trial by jury of any issues so triable by right.

Dated: October 25, 2021

Respectfully submitted,

/s/Brett E. Cooper

Brett E. Cooper (NY SBN 4011011)

bcooper@raklaw.com

Reza Mirzaie (CA SBN 246953)

rmirzaie@raklaw.com

Marc A. Fenster (CA SBN 181067)

mfenster@raklaw.com

Seth Hasenour (TX SBN 24059910)

shasenour@raklaw.com

Drew B. Hollander (NY SBN 5378096)

dhollander@raklaw.com

RUSS AUGUST & KABAT

12424 Wilshire Blvd. 12th Floor

Los Angeles, CA 90025

Phone: (310) 826-7474

Facsimile: (310) 826-6991

*Attorneys for Plaintiff Aire Technology
Limited*