EXHIBIT A

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

TELCOM VENTURES LLC, Plaintiff, v. SAMSUNG ELECTRONICS, CO., LTD. and SAMSUNG ELECTRONICS AMERICA, INC., Defendants.	Case Nos. 2:24-cv-00691-JRG JURY TRIAL DEMANDED

SAMSUNG'S FIRST AMENDED P.R. 3-3 AND 3-4 INVALIDITY CONTENTIONS

I. INTRODUCTION

Defendants Samsung Electronics, Co., Ltd. and Samsung Electronics America, Inc. (collectively, "Samsung") provide these Invalidity Contentions to Plaintiff Telcom Ventures LLC ("Telcom") for the following patents (collectively, "Asserted Patents") and claims (collectively, "Asserted Claims"), which were identified as asserted in Telcom's Preliminary Infringement Contentions served on November 21, 2024 ("Infringement Contentions"):

U.S. Patent No.	Asserted Claims
9,462,411 ("'411 patent")	All: **1**, 2, **3**, 4
9,832,708 ("'708 patent")	All: **1**, 2, 3, 4, 5, 6, 7, 8, 9, 10, **11**, 12, 13, 14, 15, **16**, 17, **18**, 19
10,219,199 ("'199 patent")	All: **1**, 2, 3, 4, 5, 6, 7, 8, 9, **10**, 11, 12, 13, 14, 15, 16, 17, 18, 19
10,674,432 ("'432 patent")	All: **1**, 2, 3, 4, 5, 6, 7, 8, 9, **10**, 11, 12, 13, 14, 15, 16, 17
11,770,756 ("'756 patent")	All: **1**, 2, 3, 4, 5, **6**, 7, 8, 9, 10, **11**, 12, 13, **14**, 15, 16, 17, 18
11,924,743 ("'743 patent")	All: **1**, 2, 3, 4, 5, 6, 7, **8**, 9, 10, 11, 12, 13, 14
11,937,172 ("'172 patent")	All: **1**, 2, 3, 4, 5, 6, 7, 8, **9**, 10, 11, 12, 13, 14, 15, 16
12,028,793 ("'793 patent")	All: **1**, 2, 3, 4, **5**, 6, 7, 8, 9, 10, 11

II. RESERVATIONS AND EXPLANATIONS

These Invalidity Contentions and accompanying document productions are subject to further revision as follows. Nothing in these contentions constitutes an admission concerning the priority date, conception date, or date of reduction to practice of the Asserted Claims. Samsung

reserves the right to modify or supplement these Invalidity Contentions, including in response to any positions taken or information disclosed regarding the priority date, conception date, or date of reduction to practice of the Asserted Claims.

This disclosure is directed to invalidity issues only and does not address other defenses or grounds, including but not limited to: claim construction, non-infringement, patent misuse, inequitable conduct, estoppel, waiver, acquiescence, patent exhaustion, unfair competition, unclean hands, express or implied license, or non-statutory defenses of any sort. Samsung reserves all rights with respect to such issues, including but not limited to their position that the Asserted Claims are to be construed in a particular manner and are not infringed.

For prior art patents and prior art publications identified in these Invalidity Contentions, Samsung reserves the right to rely on the public use, offer for sale, sale, and/or actual products embodying the methods and systems described therein uncovered during discovery. Samsung also reserves the right to rely on any related patents and patent applications, foreign patent counterparts and foreign patent applications of U.S. patents identified in these Invalidity Contentions, and U.S. counterparts of foreign patents and foreign patent applications identified in these Invalidity Contentions.

Samsung also contends that the Asserted Patents are invalid in view of public knowledge and uses and/or offers for sale or sales of products and services that are under 35 U.S.C. § 102(a) and/or 35 U.S.C. § 102(b) and/or prior inventions made in this country by other inventors who had not abandoned, suppressed, or concealed them under 35 U.S.C. § 102(g).

Samsung also reserves the right to rely on any system, public knowledge or use embodying or otherwise incorporating any of the prior art disclosed herein alone or in combination. Samsung further reserves the right to rely on any other documents or references describing any such system,

knowledge, or use. Samsung also reserves the right to rely on physical exemplars of these prior art systems (and will make the same available for inspection).

Samsung's Invalidity Contentions are based in part on Samsung's present understanding of the Asserted Claims and Telcom's apparent interpretation of these claims as reflected in its Infringement Contentions. By including prior art that anticipates or renders obvious claims based on Telcom's apparent or explicit claim interpretations, Samsung is not agreeing that Telcom's claim interpretations are correct. Any invalidity analysis depends on claim construction, which is a question of law reserved for the Court. Samsung reserves the right to amend, supplement, or materially modify its Invalidity Contentions in response to any claim construction positions that Telcom may take in this case or any claim construction the Court may adopt in this case. Samsung also reserves the right to assert that a claim is indefinite, not enabled, or fails to meet the written description requirement, in response to any additional claim construction positions Telcom may take in this case or any further claim construction the Court may adopt in this case.

Samsung contends that Telcom appears to be pursuing overly broad constructions of the Asserted Claims in an effort to piece together an infringement claim where none exists and to accuse products that do not practice the claims as properly construed. At the same time, Telcom's Infringement Contentions are in many respects too general and vague to discern exactly how Telcom contends the accused instrumentalities practice each element of the Asserted Claims. These Invalidity Contentions are not intended to be, and are not, an admission that the Asserted Claims are infringed by any of Samsung's products or technology, that any particular feature or aspect of the accused instrumentalities practices any element of the Asserted Claims, or that any of Telcom's proposed constructions are supportable or proper. To the extent that any of the prior art references disclose the same functionality or feature of any of the accused instrumentalities,

Samsung reserves the right to argue that said feature or functionality does not practice the Asserted Claims, and to argue, in the alternative, that if said feature or functionality is found to practice the Asserted Claims, then the prior art reference demonstrates that that feature or functionality is not novel, is obvious, or is not patentable.

The accompanying invalidity claim charts provide examples of prior art that discloses, either expressly or inherently, every limitation of certain claims and/or teachings, suggestions and motivations through which a POSITA at the time of the alleged invention would have considered the limitations obvious in view of the state of the art at the time, the differences between the claimed invention and the state of the art, and the foreseeability from a technical perspective and/or marketing and/or natural and expected evolution of the art. Where Samsung cites to a particular figure in a reference, the citation should be understood to encompass the caption and description of the figure and any text relating to the figure. Conversely, where Samsung cites to particular text referring to a figure, the citation should be understood to include the figure as well. As discovery progresses and the scope and focus of the liability issues become clearer, Samsung may rely on uncited portions of the prior art.

Samsung reserves the right to revise its contentions concerning the invalidity of the Asserted Claims, which may change depending on discovery taken in the case, the Court's construction of the Asserted Claims, any findings as to the priority date of the Asserted Claims, and/or positions that Telcom or expert witness(es) may take concerning claim construction, infringement, and/or invalidity issues.

Samsung may rely on Telcom's or any inventor's admissions concerning the scope of prior art relevant to the Asserted Patents; the patent prosecution histories for the Asserted Patents; any deposition testimony of the named inventors on the Asserted Patents; and the papers filed and any

evidence submitted by Telcom in connection with this litigation. For example, Samsung reserves the right to assert that the Asserted Claims are invalid under 35 U.S.C. § 102(f) in the event that Samsung obtains evidence that the named inventors did not invent (either alone or in conjunction with others) the subject matter claimed in the Asserted Patents. Should Samsung obtain such evidence, it will provide the name(s) of the person(s) from whom and the circumstances under which the claimed invention or any part of it was derived.

Prior art not included in this disclosure, whether known or not known to Samsung, may become relevant. In particular, Samsung is currently unaware of the extent, if any, to which Telcom will contend that limitations of the Asserted Patents are not disclosed in the prior art identified by Samsung. To the extent such an issue arises, Samsung reserves the right to identify other references that would render obvious the allegedly missing limitation(s) of the disclosed device or method. Further, because Samsung has not yet completed its search for or analysis of relevant prior art, Samsung reserves the right to revise, amend, and/or supplement the information provided herein, including identifying, charting, and relying on additional references, should Samsung's further search and analysis yield additional information or references, consistent with the Federal Rules of Civil Procedure. Plaintiff also has a duty to produce to Defendants all relevant documents from other proceedings involving the patents related to the asserted patents or their subject matter, including but not limited to all prior art invalidity contentions and expert reports on invalidity among other relevant items.

Additionally, because third-party discovery is not yet complete, Samsung reserves the right to present additional items of prior art under 35 U.S.C. §§ 102(a), (b), (e), and/or (g), and/or § 103, located during the course of such discovery or further investigation, and to assert invalidity under 35 U.S.C. §§ 102(c), (d), or (f), to the extent that such discovery or investigation yields information

forming the basis for such invalidity. For example, Samsung has issued or plans to issue subpoenas to (and has received and expects to receive, voluntarily or subject to subpoenas, information from) third parties believed to have knowledge, documentation, and/or corroborating evidence concerning some of the prior art listed below and/or additional prior art. These third parties include, without limitation, the authors, inventors, vendors, or assignees of the references listed in these disclosures.

Samsung further reserve the right to modify or add additional contentions in the event that Telcom provides amended infringement contentions and to the extent the Court orders or allows Telcom to amend its infringement contentions.

Pursuant to the Scheduling Order, and in light of Telcom's Infringement Contentions and accompanying claim chart, Samsung lists in these Invalidity Contentions the prior art now known to it that it contends anticipates or renders obvious the Asserted Claims. Although Samsung has identified at least one disclosure of a limitation for each prior art reference, each and every disclosure of the same limitation in the same reference is not necessarily identified. In an effort to focus the issues, Samsung's citations are only to representative portions of an identified reference, even where a reference may contain additional support for a particular claim limitation. POSITAs generally read an item of prior art as a whole and in the context of other publications and literature. Thus, to understand and interpret any specific statement or disclosure within a prior art reference, such persons would rely on other information within the reference, along with other publications and their general scientific knowledge. Samsung may rely on uncited portions of the prior art references and on other publications and expert testimony to provide context, and as aids to understanding and interpreting the portions that are cited.

Samsung incorporates in these Invalidity Contentions, in full, all prior art references cited in the Asserted Patents and their prosecution histories.

Subject to Samsung's reservation of rights, Samsung identifies each item of prior art that anticipates and/or renders obvious the Asserted Claims. The patents/applications, publications, and systems identified are also relevant to show the state of the art and reasons and motivations for making improvements, additions, and combinations.

III. PRIORITY DATE OF THE ASSERTED PATENTS AND CLAIMS

Telcom asserts that the Asserted Claims are each entitled to a priority date of November ~~8~~4, 2008. (Infringement Contentions, p. 6).

It is Telcom's burden to show entitlement to its asserted priority date, and Samsung asserts that Telcom has failed to meet that burden. *See Tech. Licensing Corp. v. Videotek, Inc.*, 545 F.3d 1316, 1327 (Fed. Cir. 2008); *see also, In re Magnum Oil Tools Int'l, Ltd.*, 829 F.3d 1364, 1376 (Fed. Cir. 2016) ("[A] patentee bears the burden of establishing that its claimed invention is entitled to an earlier priority date than an asserted prior art reference."). For example, Telcom has failed to show that Asserted Claims in divisional and continuation patents are supported by the parent application that resulted in the allowed '411 patent (Application No. 12/264,711), to which they all ultimately claim priority.

Nevertheless, Samsung has focused on prior art that predates the claimed priority date. Samsung reserves the right to amend these Invalidity Contentions with additional prior art and/or with additional charts of the art if Telcom alleges earlier or later priority dates.

In addition, Telcom has not identified a date of conception or reduction to practice for the Asserted Patents, other than producing the file histories for those patents and identifying them as "related to the conception and reduction to practice of each Asserted Patent" on page 7 of its Infringement Contentions. Samsung therefore also reserves its right to amend its Invalidity

Contentions if Telcom is permitted to allege earlier dates of conception for the patents-in-suit, or if Telcom does not meet its burden to prove the priority dates it asserts.

IV. PRIOR ART REFERENCES

Samsung identifies the following prior art now known to Samsung to anticipate or render obvious the Asserted Claims under at least 35 U.S.C. §§ 102(a), (b), (e), and/or (g), either expressly or inherently as understood by a POSITA, and/or render obvious under 35 U.S.C. § 103, either alone or in combination. At this time, Samsung contends that the prior art references described below anticipate or render obvious, either alone or in combination, one or more of the Asserted Claims. These prior art references also provide a description of the level of skill in the art and provide background information showing the knowledge of a person of skill in the art. Samsung reserves the right to rely on these references for those purposes.

Samsung additionally incorporates by reference all prior art references cited on the face of the Asserted Patents, each related patent, and each foreign counterpart. Samsung further incorporates by reference all prior art references identified in the file histories of the same. Samsung reserves the right to rely upon foreign counterparts of the U.S. Patents identified in these Invalidity Contentions; U.S. counterparts of foreign patents and foreign patent applications identified in these Invalidity Contentions; U.S. and foreign patents and patent applications corresponding to articles and publications identified in these Invalidity Contentions; and any systems, products, or prior inventions related to any references identified in these Invalidity Contentions.

In these Invalidity Contentions, including the exhibits, any citation to a printed publication or other reference describing a prior art system should also be construed to include a reference to the prior art system itself.

Each Asserted Patent has asserted claims with limitations that are substantially similar to limitations of other asserted claims of that Asserted Patent. Each Asserted Patent also has asserted claims with limitations that are substantially similar to limitations of asserted claims on other Asserted Patents. For example, many of the asserted claims recite a "smartphone," recite "air interfaces" with various properties, recite sensing physiological input and detected proximity, recite a similar sequence of obtaining authorizations and conditionally enabling or disabling functionality based on the sensed input and/or the detected proximity, etc. Samsung reserves the right to rely on references and obviousness arguments charted for a limitation of one asserted claim when invalidating another asserted claim with a similar limitation.

Similarly, these Invalidity Contentions, including the exhibits, may contain citations to certain embodiments disclosed in a prior art reference but not to all embodiments disclosed in that reference. Samsung reserves the right to rely on variant embodiments in cited prior art references even if those variant embodiments are not otherwise specifically cited.

A. Prior Art Patents and Publications

Prior Art	Effective Filing Date	Publication / Issue Date	Country of Origin
CA2335532 (De Schrijver)	1999-06-26	2000-01-06	Canada
CA2466734 (Samar)	2003-01-22	2003-07-31	Canada
CA2467591 (Xydis)	2001-11-29	2003-06-12	Canada
EP1016999 (Ogasawara)	1999-07-05	2000-07-05	EPO
EP1224518 (Vamvakas)	2000-10-06	2009-07-15	EPO
EP1470534 (Samar)	2003-01-22	2004-10-27	EPO
EP1536306 ('306 Buer)	2004-09-30	2005-06-01	EPO
EP1864467 (Vesikivi)	2006-03-27	2007-12-12	EPO
EP1959369 (Takashi)	1999-12-10	2008-08-20	EPO
EP2064649 (Lahdenniemi)	2006-09-20	2009-06-23	EPO
EP2099203 (Dietz)	2008-03-06	2009-09-09	EPO
EP2797020 Buer)	2004-09-30	2014-10-29	EPO
EP2937805 (Buer)	2004-09-30	2015-10-28	EPO
EP3023899 (Buer)	2004-09-30	2006-05-25	EPO

GB2353386 (Scott)	1999-04-26	1999-11-04	Great Britain
GB2401462 (Chen)	2004-04-22	2004-11-10	Great Britain
JP2001273451 (Aoki)	2000-03-28	2001-10-05	Japan
JP2002366988 (Nakai)	2001-06-11	2002-12-20	Japan
JP2005524181 (Yeo)	2003-04-29	2005-08-11	Japan
JP2006050466 (Junji)	2004-08-06	2449-03-27	Japan
JP2006352325 (Hiroto)	2005-06-14	2006-12-28	Japan
JP2007036693 (Ohashi)	2005-07-27	2007-02-08	Japan
JP2007150668 (Ikeda)	2005-11-28	2007-06-14	Japan
JP2007257666 (Ueda)	2007-06-18	2097-10-04	Japan
KR100778367 (Choi)	2006-08-02	2007-11-22	Republic of Korea
KR20030093464 (Ho-seong)	2002-06-03	2003-012-11	Republic of Korea
KR20060048692 (Chang)	2005-06-29	2006-05-18	Republic of Korea
KR20070022422 (Min)	2005-08-22	2007-02-27	Republic of Korea
KR20070109508 (Kwon)	2006-05-11	2007-11-15	Republic of Korea
US20010000535 (Lapsley)	2000-12-06	2001-04-26	USA
US20010022805 (Dabak 805)	2001-02-26	2001-05-21	USA
US20010026632 (Tamai)	2001-03-19	2001-10-04	USA
US20010030644 (Allport)	2001-06-05	2001-10-18	USA
US20020003892 (Iwanaga)	2001-07-09	2002-01-10	USA
US20020046336 (Kon)	2001-08-30	2002-04-18	USA
US20020099665 (Burger)	2001-10-01	2002-07-25	USA
US20020109580 (Shreve)	2001-02-13	2002-08-15	USA
US20020116508 (Khan)	2002-02-20	2002-08-22	USA
US20020126780 (Oshima)	2001-12-05	2002-09-12	USA
US20020170961 (Dickson)	2001-05-17	2002-11-21	USA
US20020188574 (Niwa)	2002-07-29	2002-12-12	USA
US20020194128 (Maritzen)	2002-03-27	2002-12-19	USA
US20030025603 (Smith 603)	2001-08-01	2003-02-06	USA
US20030037264 (Ezaki)	2002-08-13	2003-02-20	USA
US20030051138 (Maeda)	2002-06-24	2003-03-13	USA
US20030055792 (Kinoshita)	2001-07-23	2003-03-20	USA
US20030074317 (Hofi)	2001-10-15	2003-04-17	USA
US20030093693 (Blight)	2003-11-12	2003-05-15	USA
US20030120934 (Ortiz)	2001-01-10	2010-09-07	USA
US20030131114 (Scheidt)	2002-10-15	2003-07-10	USA

US20030135740 (Talmor)	2001-09-05	2003-07-17	USA
US20030140233 (Samar)	2002-01-22	2003-07-24	USA
US20030154382 (Vicard)	2003-01-17	2003-08-14	USA
US20030177102 (Robinson)	2001-09-21	2003-09-18	USA
US20030196084 (Okereke)	2003-04-11	2003-10-16	USA
US20030200446 (Siegel)	2002-04-19	2003-10-23	USA
US20030220876 (Burger)	2003-03-19	2003-11-27	USA
US20040002902 (Muehlhaeuser)	2003-03-03	2004-01-01	USA
US20040014423 (Croome)	2003-05-14	2004-01-22	USA
US20040044627 (Russell)	2000-11-29	2004-03-04	USA
US20040123106 (D'Angelo)	2003-08-26	2004-06-24	USA
US20040148526 (Sands)	2003-01-24	2004-07-29	USA
US20040153649 (Rhoads)	1995-07-27	2010-08-03	USA
US20040255139 (Giobbi)	2000-12-27	2007-12-04	USA
US20040257196 (Kotzin)	2003-06-20	2004-12-23	USA
US20050005136 (Chen)	2004-04-21	2005-01-06	USA
US20050039027 (Shapiro)	2003-07-25	2005-02-17	USA
US20050091213 (Schutz)	2003-10-23	2005-04-28	USA
US20050105734 (Buer)	2004-09-30	2005-05-19	USA
US20050137977 (Wankmueller)	2004-09-27	2005-06-23	USA
US20050218215 (Lauden)	2005-03-31	2005-10-06	USA
US20050221798 (Sengupta 798)	2004-03-30	2005-10-06	USA
US20050221798 (Sengupta)	2004-03-30	2005-10-06	USA
US20050222961 (Staib)	2004-09-14	2005-10-06	USA
US20050225430 (Seifert)	2002-12-19	2005-10-13	USA
US20050253683 (Lowe)	2004-05-17	2005-11-17	USA
US20050269401 (Spitzer)	2005-06-03	2005-12-08	USA
US20050273440 (Ching)	2005-05-13	2005-12-08	USA
US20060080525 (Ritter)	2005-10-11	2006-04-13	USA
US20060081714 (King)	2005-08-23	2006-04-20	USA
US20060129838 (Chen)	2002-08-08	2006-06-15	USA
US20060136717 (Buer)	2005-08-15	2006-06-22	USA
US20060136741 (Mercredi)	2004-12-16	2006-06-22	USA
US20060142058 (Elias)	2006-02-17	2006-06-29	USA
US20060143441 (Giobbi 441)	2005-12-12	2006-06-29	USA
US20060165060 (Dua)	2005-01-21	2006-07-27	USA
US20060204048 (Morrison)	2005-03-25	2006-09-14	USA
US20060248554 (Priddy)	2006-06-27	2006-11-02	USA
US20070008066 (Fukuda)	2004-05-19	2007-01-11	USA

US20070038867 (Verbauwhede)	2004-06-02	2007-02-15	USA
US20070057763 (Blattner)	2005-09-12	2007-03-15	USA
US20070075965 (Huppi)	2006-10-24	2007-04-05	USA
US20070108269 (Benco)	2005-11-16	2007-05-17	USA
US20070124211 (Smith 211)	2006-05-25	2007-05-31	USA
US20070156436 (Fisher 436)	2006-08-25	2007-07-05	USA
US20070156436 (Fisher)	2006-08-25	2007-07-05	USA
US20070198436 (Weiss)	2007-02-21	2007-08-23	USA
US20070245157 (Giobbi)	2007-05-07	2007-10-18	USA
US20070245158 (Giobbi)	2007-05-07	2007-10-18	USA
US20070260883 (Giobbi)	2007-05-05	2007-11-08	USA
US20070270128 (Kakiuchi)	2007-03-15	2007-11-22	USA
US20080022089 (Leedom)	2006-06-26	2008-01-24	USA
US20080046366 (Bemmel)	2006-12-05	2008-02-21	USA
US20080052192 (Fisher 192)	2007-10-31	2008-02-28	USA
US20080085743 (Klinghult)	2006-10-20	2008-04-10	USA
US20080097855 (Rissanen)	1999-12-15	2008-04-24	USA
US20080100414 (Diab)	2006-10-30	2008-05-01	USA
US20080114699 (Yuan)	2007-10-29	2008-05-15	USA
US20080122582 (Baker)	2006-11-29	2008-05-29	USA
US20080140868 (Kalayjian)	2006-12-12	2008-06-12	USA
US20080147546 (Weichselbaumer 546)	2006-10-10	2008-06-19	USA
US20080150678 (Giobbi)	2007-11-13	2008-06-26	USA
US20080167000 (Wentker 000)	2008-01-09	2008-07-10	USA
US20080220752 (Forstall)	2007-06-28	2008-09-11	USA
US20080313082 (Van Bosch)	2007-06-14	2008-12-18	USA
US20090024525 (Blumer)	2008-07-16	2009-01-22	USA
US20090037326 (Chitti)	2008-02-29	2009-02-05	USA
US20090065575 (Phillips 575)	2007-09-10	2009-03-12	USA
US20090068982 (Chen 982)	2007-09-10	2009-03-12	USA
US20090069049 (Jain 049)	2008-09-05	2009-03-12	USA
US20090070272 (Jain 272)	2007-09-12	2009-03-12	USA
US20090083947 (Fadell)	2008-09-09	2009-03-26	USA
US20090094681 (Sadler)	2007-10-03	2009-04-09	USA
US20090112766 (Hammad 766)	2008-10-23	2009-04-30	USA
US20090117919 (Hershenson)	2002-10-01	2009-05-07	USA
US20090124234 (Fisher 234)	2007-11-14	2009-05-14	USA
US20090143104 (Loh)	2007-09-21	2009-06-04	USA
US20090144161 (Fisher 161)	2007-11-30	2009-06-04	USA

US20090192912 (Griffin 912)	2008-09-30	2009-07-30	USA
US20090192935 (Griffin 935)	2008-09-30	2009-07-30	USA
US20090210308 (Toomer)	2008-02-15	2009-08-20	USA
US20090215385 (Waters)	2005-02-15	2009-08-27	USA
US20090271276 (Roberts)	2008-04-24	2009-10-29	USA
US20090294523 (Marano)	2006-01-03	2009-01-03	USA
US20090307140 (Mardikar 140)	2008-10-10	2009-12-10	USA
US20100022254 (Ashfield)	2008-07-22	2010-01-28	USA
US20100049987 (Ettorre)	2006-12-19	2010-02-25	USA
US20100062743 (Jonsson)	2004-08-20	2010-03-11	USA
US20100082481 (Lin 481)	2008-09-30	2010-04-01	USA
US20100082490 (Rosenblatt 490)	2008-09-30	2010-04-01	USA
US20100088188 (Kumar 188)	2008-10-06	2010-04-08	USA
US20100145850 (Nagai)	2008-04-15	2010-06-10	USA
US20190080320 (Hammad 320)	2018-11-13	2019-03-14	USA
US20190244188 (Fisher 188)	2019-04-20	2019-08-08	USA
US3713148 (Cardullo)	1970-05-21	1973-01-23	USA
US3752960 (Walton)	1905-05-24	1973-08-14	USA
US5623552 (Lane)	1994-08-15	1997-04-22	USA
US5708422 (Blonder)	1995-05-31	1998-01-13	USA
US5867795 (Novis)	1996-08-23	1999-02-02	USA
US6011858 (Stock)	1996-05-10	2000-01-04	USA
US6016476 (Maes)	1998-01-16	2000-01-18	USA
US6041410 (Hsu)	1997-12-22	2000-03-21	USA
US6104922 (Baumann)	1998-03-02	2000-08-15	USA
US6219439 (Burger)	1998-07-09	2001-04-17	USA
US6325285 (Baratelli)	1999-11-12	2001-12-04	USA
US6353889 (Hollingshead)	1998-05-13	2002-03-05	USA
US6751734 (Uchida)	2000-03-21	2004-06-15	USA
US6774796 (Smith 796)	2001-08-01	2003-02-06	USA
US6819219 (Bolle)	2000-10-12	2004-11-16	USA
US6907135 (Gifford)	1999-03-02	2005-06-14	USA
US6937135 (Kitson)	2001-05-30	2005-08-30	USA
US6957339 (Shinzaki)	2002-06-07	2005-10-18	USA
US6957339 (Shinzaki)	2002-06-07	2005-10-18	USA
US7058114 (Dabak 114)	2001-02-26	2001-09-20	USA
US7124937 (Myers)	2005-01-21	2006-10-24	USA
US7155416 (Shatford)	2003-07-03	2006-12-26	USA
US7174031 (Rhoads)	2005-05-17	2007-02-06	USA

US7188110 (Ludtke)	2000-12-11	2007-03-06	USA
US7200755 (Hamid)	2001-05-24	2007-04-03	USA
US7249112 (Berardi)	2002-12-13	2007-07-24	USA
US7310042 (Seifert)	2004-12-19	2007-12-18	USA
US7340439 (Burger)	2003-03-19	2008-03-04	USA
US7376583 (Rolf)	2000-08-10	2008-05-20	USA
US7378939 (Sengupta 939)	2004-03-30	2005-10-06	USA
US7404086 (Sands)	2003-01-24	2008-07-22	USA
US7428507 (Villaret)	2001-06-29	2008-09-23	USA
US7478065 (Ritter 065)	1999-12-23	2009-01-13	USA
US7478065 (Ritter)	1999-12-23	2009-01-13	USA
US7561691 (Blight)	2001-11-12	2009-07-14	USA
US7636854 (Müller)	2002-05-02	2009-12-22	USA
US7690577 (Beenau)	2007-09-20	2010-04-06	USA
US7694331 (Vesikivi)	2005-04-01	2010-04-06	USA
US7707113 (DiMartino 113)	2007-09-28	2010-04-27	USA
US7719422 (Steinmetz)	2007-08-30	2010-05-18	USA
US7766223 (Mello)	2007-11-08	2010-08-03	USA
US7784684 (Labrou)	2006-07-18	2010-08-31	USA
US7909243 (Merkow)	2007-08-28	2011-03-22	USA
US7962369 (Rosenberg)	2007-10-01	2011-06-14	USA
US7988058 (Englebardt)	2008-01-25	2011-08-02	USA
US7992779 (Phillips 779)	2007-09-10	2009-03-12	USA
US7997476 (Gannon)	2005-09-15	2011-08-16	USA
US8055581 (Royyuru 581)	2007-02-22	2011-11-08	USA
US8126806 (DiMartino 806)	2007-12-03	2012-02-28	USA
US8135647 (Hammad 647)	2007-06-14	2008-01-03	USA
US8150772 (Mardikar 772)	2008-06-09	2012-04-03	USA
US8166523 (Ezaki)	2002-08-13	2012-04-24	USA
US8200980 (Robinson)	2004-06-07	2012-06-12	USA
US8232862 (Lowe)	2004-05-17	2012-07-31	USA
US8249935 (DiMartino)	2007-09-27	2012-08-21	USA
US8285329 (Zhu)	2007-04-02	2012-10-09	USA
US8286862 (Phillips 862)	2007-12-28	2012-10-16	USA
US8332323 (Stalls)	2008-12-04	2012-12-11	USA
US8333317 (Buer)	2004-09-30	2012-12-18	USA
US8341088 (Boutahar)	2004-06-30	2012-12-25	USA
US8395478 (Diab)	2006-10-30	2013-03-12	USA
US8468095 (DiMartino 095)	2007-12-03	2013-06-18	USA

US8469277 (Johnson)	2006-12-19	2008-01-31	USA
US8543496 (Beenau 496)	2007-04-27	2013-09-24	USA
US8548927 (Beenau)	2001-07-10	2013-10-01	USA
US8565723 (Cox)	2007-10-17	2013-10-22	USA
US8594563 (Waters)	2005-02-15	2013-11-26	USA
US8620260 (Beenau 260)	2007-04-27	2013-12-31	USA
US8657203 (Diamond 203)	2008-08-14	2014-02-25	USA
US8662401 (Skowronek)	2008-07-25	2014-03-04	USA
US8712429 (Nagorniak)	2008-09-11	2010-03-11	USA
US8893284 (Sadler)	2007-10-03	2014-11-18	USA
US8923827 (Wentker 827)	2008-01-09	2008-07-10	USA
US8955083 (Ettorre)	2006-12-19	2015-02-10	USA
US8989712 (Wentker 712)	2008-01-09	2008-07-10	USA
US9042819 (Dua)	2005-05-12	2015-01-15	USA
US9082267 (Rosenberg)	2007-10-01	2015-07-14	USA
US9269221 (Gobbi)	2007-11-13	2016-02-23	USA
US9286606 (Diamond 606)	2008-08-14	2016-03-15	USA
US9401063 (Foran-Owens)	2007-12-13	2016-07-26	USA
US9542542 (Giobbi)	2007-05-07	2017-01-10	USA
US9552584 (Bierbaum)	2011-04-28	2017-01-24	USA
US9558485 (Griffin 485)	2008-09-30	2009-07-30	USA
US9672508 (Aabye 508)	2008-09-22	2017-06-06	USA
US9824355 (Aabye 355)	2008-09-22	2017-11-21	USA
US9846866 (Royyuru 866)	2007-02-22	2017-12-19	USA
US10026076 (Kumar 076)	2008-10-06	2018-07-17	USA
US10057085 (Wentker 0085)	2008-01-09	2008-07-10	USA
US10380573 (Lin 573)	2008-09-30	2010-04-01	USA
US10600045 (Shenker)	2018-06-22	2018-10-18	USA
US11790332 (Jones)	2019-01-17	2019-05-23	USA
WO1990006633 (Lee)	1988-12-09	1990-06-14	WIPO
WO1998012670 (Borza)	1997-09-15	1998-03-26	WIPO
WO1999056429 (Scott)	1999-04-26	1999-11-04	WIPO
WO2000000882 (De Schrijver)	1999-06-25	2000-01-06	WIPO
WO2000000923 (Valliani)	1999-06-30	2000-01-06	WIPO
WO2001073575 (Smith 575)	2001-03-27	2001-10-04	WIPO
WO2001027723 (Vamvakas)	2000-10-06	2001-04-19	WIPO
WO2002049322 (Holloway)	2001-12-11	2002-06-20	WIPO
WO2002089018 (Pu)	2001-05-02	2002-11-07	WIPO
WO2002095547 (Hamid)	2002-04-23	2002-11-28	WIPO

WO2003003295 (Poo)	2001-06-28	2003-01-09	WIPO
WO2003036861 (Black)	2002-05-28	2003-05-01	WIPO
WO2003054806 (Seifert)	2002-12-19	2003-07-03	WIPO
WO2003063094 (Samar)	2002-01-22	2003-07-31	WIPO
WO2003093923 (Eryou)	2003-04-30	2003-11-13	WIPO
WO2004019190 (Chen)	2002-08-08	2004-03-04	WIPO
WO2004068283 (Sands)	2004-01-23	2004-08-12	WIPO
WO2006087503 (Waters 503)	2005-02-15	2006-08-24	WIPO
WO2007109574 (Alberth 574)	2007-03-16	2007-09-27	WIPO
WO2007133037 (Lee)	2007-11-22	2007-11-22	WIPO
WO2007133541 (Giobbi)	2007-05-07	2007-11-22	WIPO
WO2008014321 (Sally)	2007-07-25	2008-01-31	WIPO

Prior Art	Author	Pub. Date	Publisher
Secure cash withdrawal through mobile phone/device	A. Arabo	2008	
A review of OFDMA and single-carrier FDMA	C. Ciochina and H. Sari	2010	
iPhone Premieres This Friday Night at Apple Retail Stores		2007-06-28	Apple
Near Field Communication in the real world		2006	Innovision
Parasitic Authentication To Protect Your E-Wallet	P. Thorne, T. Ebringer and Y. Zheng,	2000	Computer
Security Issues in Mobile Payment Systems	Agarwal, Shivani, Mitesh Khapra, Bernard L. Menezes and Nirav Uchat.	2007	
Smart Spaces with Real-Time Physiological Measurement and Mitigation of Stress	R. G. Cooper, J. Al-Muhtadi and R. Ashford,	Oct-08	
T-Mobile Unveils the T-Mobile G1 — the First Phone Powered by Android		2008-09-23	T-Mobile
A sampling of NFC pilots from around the world	Zack Martin	2007-05-31	SecureIDNews

Public Key Infrastructure (PKI) Interoperability: A Security Services Approach to Support Transfer of Trust	A. Hansen	1999-09	
Handbook of Applied Cryptography	A. Menezes	1996	
Nonmonotonic Cryptographic Protocols	A. Rubin	1994	
An Introduction to Near-Field Communication and the Contactless Communication API	C . Enrique Ortiz	2008-06	Oracle
Authenticating Users on Handheld Devices	Wayne A. Jansen	2003-05-01	NIST
Beyond Fingerprinting: Is Biometrics the Best Bet for Fighting Identity Theft?	Jain and Pankanti	2008-09	Scientific American
Biometrics – Rising to the challenge of technology innovation	Fernando L. Podio	2006-02	ISO Focus
BlackBerry 8820 (T-Mobile) review	Bonnie Cha	2008-03-23	CNET
Bradford 2007 Speech	Terri Bradford	2007-09	Federal Reserve Bank of Kansas City
Internet X.509 Public Key Infrastructure Certificate Management Protocols	C. Adams	1999-03	
Caen France hosts world's premier NFC trial with mobile phones enabling host of contactless applications	Chris Corum	2005-11-23	SecureIDNews
Call t E-ZPass The Hard Way	John Sullivan	2001-09-09	The New York Times
Calypso Wireless Successfully Demonstrated the C1250i Wi-Fi-GSM VoIP Skype Call Connectivity Cellular Phones on Vodafone Network at 3GSM Congress		2006-02-27	Calypso Wireless
Cards for all seasons	Chris Stanford	2006-02	ISO Focus
Series X: Data Communication Networks: The Directory – Authentication Framework		1988-11	CCITT
Cell Phone Thumbprint Sensor		2003-07-22	Blog.greggman.com
Complex landscapes: mobile payments in Japan, South Korea, and the United States	Bradford & Hayashi	2007-09	Federal Reserve Bank of Kansas City

Contactless Payment and the Retail Point of Sale: Applications, Technologies and Transaction Models		2003-03	Smart Card Alliance
Contactless: the next payment wave?	Terri Bradford	2005-12	Federal Reserve Bank of Kansas City
Trusted Third Party Services for Deploying Secure Telemedical Applications over the WWW	D. Spinellis	1999	
Developing Practical Wireless Applications	Gratton	2007	Elsevier
Discover Network And Motorola Announce Mobile Payments And Account Management Trial		2007-02-13	Discover
Discover Teaming With Motorola on NFC, Mobile-Banking Trial	Mary Catherine O'Connor	2007-02-14	RFiD Journal
Eleven Companies Collaborate to Promote the 'Edy' Prepaid Electronic Money Service for the IT Era		2000-12-25	Sony
RFID and Identity Management in Everyday Life		2006	European Parliament Scientific Technology Options Assessment
Exxon Mobil 2001 Summary Annual Report	ExxonMobil	2002	ExxonMobil
Exxon Mobil Form 8-K/A	ExxonMobil	2005-03-17	ExxonMobil
ExxonMobil Expands the Speedpass System to More Than 2,500 Exxon-brandedService Stations	ExxonMobil	2001-08-01	ExxonMobil
Authentication in an Electronic Banking Environment (FFIEC)		2001-08-08	Federal Financial Institutions Examination Council
Federal Information Processing Standard (FIPS) Publication 46, The Data Encryption Standard (DES)		1977	Nat'l Institute of Standards and Technology
Fingerprint Recognition		2006	NSTC Subcommittee on Biometrics

			and Identity Management
The Standard for Smart Card Infrastructure: Concise Guide to Worldwide Implementation of GlobalPlatform Technology		2006	GlobalPlatform
GSM Association Aims for Global Point of Sale Purchases by Mobile Phone		2007-02-13	The GSM Association
Hard-to-Shop-for People on Your Holiday List? How about an Electronic Wallet for Their Wrists?	ExxonMobil	2002-12-04	ExxonMobil
HP iPaq hx2000 review: HP iPaq hx2000	Brian Nadel	2005-12-06	CNET
Wireless Access Monitoring and Control System based on Digital Door Lock	Hwang	2007	
Smart Phone: An Embedded System for Universal Interaction	Iftode	2006	
ISE/IEC 14443 Overview	Andy Richardson	2007-07	Texas Instruments
Identifying Computer Users with Authentication Devices	J.C. Spender	1987	
Japanese get first mobile wallets		2004-08-10	BBC News
KYOCERA Wireless Demonstrates Emerging Wireless Technologies at CTIA Wireless 2008		2008-04-01	Kyocera Wireless
KYOCERA Wireless Mobile Phones Excel in Cellular South WirelessWallet Consumer Trial		2007-10-18	Kyocera Wireless
KYOCERA Wireless Mobile Phones Excel in Cellular South WirelessWallet Consumer Trial		2007-10-18	Kyocera Wireless
Comparing Passwords, Tokens, and Biometrics for User Authentication	Lawrence O'Gorman	2003	
Life on the Mississippi	Mark Twain	1883	
London NFC trial shows customers want contactless m-payments		2008-09-02	Finextra
McDonald's testing e-payment system	The Associated Press	2001-05-29	USA Today
Mobil Celebrates Four Million Speedpass Customers; Innovative	ExxonMobil	2000-10-31	ExxonMobil

Payment Technology Moving Inside at C-Stores			
Mobile J/Speedy(TM) Near Field Communication Mobile Payment Pilot Project Successfully Launched in Europe by JCB Led Team		2006-10-12	JCB
Mobile Payment Adoption in the US: A Cross-Industry, Crossplatform Solution	Dewan and Chen	2005	Journal of Information Privacy and Security, Vol. 1, Issue 2.
Mobile payment: A journey through existing procedures and standardization initiatives	Karnouskos	2004-10-01	IEEE Communications Surveys & Tutorials, Vol. 6, Issue 4, 44 - 66
Momentum Builds Around GSMA's Pay-Buy Mobile Project		2007-04-25	The GSM Association
MONETA Services of SK Telecom: Lessons from Business Convergence Experiences for Ubiquitous Computing Services	Kim et al.	2004-05	Second IEEE Workshop on Software Technologies for Future Embedded and Ubiquitous Systems
A Survey of Read-Only Memories	Morton H. Lewin	1965	
Multi-Carrier and Spread Spectrum Systems: From OFDM and MC-CDMA to LTE and WiMAX, 2nd Edition	Fazel and Kaiser	2008-11-03	Wiley
Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications		2006	NFC Forum
New Isn't Necessarily Better, Especially for Cellphones	H. Asher Bolande	2002-07-12	The Wall Street Journal
New phones could replace wallets		2004-06-16	NBC News
NFC Forum News Conference		2006-06-05	NFC Forum
NFC Forum Unveils Technology Architecture And Announces Initial Specifications And Mandatory Tag Format Support		2006-06-05	NFC Forum

NFC-Trial Hagenberg		2006	NFC Research Lab Hagenberg
NFC-Trial Hagenberg: Payment		2006	NFC Research Lab Hagenberg
Modelling in Data Base Management Systems	Nijssen, G.M.,	1976	
No Cash? No Card? No Problem! - New Speedpass Features Allow Stop & Shop Customers to Pay and Save All in One	ExxonMobil	2003-02-12	ExxonMobil
Nonbanks in the payments system: European and U.S. perspectives		2007-05	Federal Reserve Bank of Kansas City
O2 NFC put to trial in the UK	Dhiram Shah	2007-11-28	New Launches
Only in Japan: The best technologies you can't buy	Martyn Williams	2008-02-11	Infoworld
Osaifu-Keitai: DoCoMo's Powerfully Convenient Mobile Wallet	Dhiram Shah	2007-06-19	Far East Gizmos
Osaifu-Keitai: iD credit payment services		2006	NTT DoCoMo
Osaifu-Keitai: What's "Osaifu-Keitai"		2006	NTT DoCoMo
Overview of Felica		Pre-2006	Sony
Trusted third parties in electronic commerce	P.J. Skevington	Apr-97	
Paper, plastic... or phone?	Terri Bradford	2006-12	Federal Reserve Bank of Kansas City
Past, present and future of mobile payments research: A literature review	Dahlberg et al.	2007-02-09	Electronic Commerce Research and Applications 7 (2008) 165–181
Pay-Buy Mobile initiative gets underway with major backing		2007-04-25	RCRWirelessNews
Payment types at the point of sale : merchant considerations	Terri Bradford	2004-12	Federal Reserve Bank of Kansas City
Payment with mobile NFC Phones: How to Analyze the Security Problems	Pasquet et al.	2008-02-16	The 2008 International Symposium on Collaborative Technologies and Systems

PayPass – M/Chip Reader Card Application Interface Specification		2008-09	MasterCard Worldwide
Performance Analysis Of OFDM	Ahamed	2008-01	Journal of Theoretical and Applied Information Technology, Vol. 4, No. 1
Policy-based Management for Body-Sensor Networks	Keoh, S.L. et al.	2007	4th International Workshop on Wearable and Implantable Body Sensor Networks
Press Kit – Speedpass	ExxonMobil	2004	ExxonMobil
Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure		2007	Smart Card Alliance
Proximity Mobile Payments Business Scenarios: Research Report on Stakeholder Perspectives		2008-07	Smart Card Alliance
Revamping the supply chain with RFID	Craig K. Harmon	2006-02	ISO Focus
RF-Based Contactless Payment Whitepaper (Version 3.0)		2006	ViVOtech
RFID – A technology whose time has come!	Steve Halliday	2006-02	ISO Focus
RFID Systems and Security and Privacy Implications	Sarma, Weis, and Engels	2003	
A Method for Obtaining Digital Signatures and Public Key Cryptosystems	Ronald Rivest, Adi Shamir, and Leonard Adleman	1978	Communications of the ACM
Samsung SCH-i730 (Verizon Wireless) review	Denny Atkin	2005-06-30	CNET
SD RFID Card	John Wehr	2005-03-15	NFCNews
Secure Payment with NFC Mobile Phone in the SmartTouch Project	Pasquet et al.	2008-06-017	IEEE: 2008 International Symposium on Collaborative Technologies and Systems
Mobile wallets start to take shape,	Shillingford	2005-03-01	BBC News business reporter

Short Range Wireless Technologies with Mobile Payment Systems	Chen	2004	
Shrouds of Time: This history or RFID	Landt	2001	Association for Automatic Identification and Data Capture Technology
Sony Felica WMV Video		Pre-2006	Sony
Speedpass Expands to More Than 400 McDonald's Restaurants in the Chicagoland Area; Now Five Million Users Strong, Proprietary Payment System Moves Beyond the Pump	ExxonMobil	2001-05-31	ExxonMobil
Speedpass Fact Sheet	ExxonMobil	2004	ExxonMobil
Speedpass FAQ	ExxonMobil	2004	ExxonMobil
Speedpass: How It Works	ExxonMobil	2004	ExxonMobil
Speedpass-enabled Timex Watch Now Available Online!	ExxonMobil	2004	ExxonMobil
Stick 'em up. A Pantech GI100? Then gimme your phone and your thumbs!	Ryan Block	2004-08-03	Engadget
Stop & Shop Teams up with Speedpass Network	ExxonMobil	2002-07-10	ExxonMobil
The Cell-Phone Revolution	Tom Farley	2007-08-22	American Heritage
The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application	Au and Kauffman	2007-01-27	Electronic Commerce Research and Applications 7 (2008) 141–164
The History of RFID Technology	Bob Violino	2005-01-16	RFiD Journal
The Magic of RFID: Just how do those little things work anyway?	Roy Want	2004-10-01	ACM Queue
The Mobil Speedpass and Mobile Commerce	Rottenberg and Liu	2002	MIT Undergraduate Research Journal, Vol. 7
T-Mobile USA Launches BlackBerry 8820		2008-03-23	T-Mobile
Toshiba Portégé G500 and G900		2007-04-10	Mobile Gazette
Toshiba Portege G900 and G500: Finger-friendly smart phones	Andrew Lim	2007-02-14	CNET

Toshiba Portege G900 review: Toshiba Portege G900	Andrew Lim	2007-07-24	CNET
New Directions in Cryptograph	Whitfield Diffie and Martin Hellman	1976	IEEE Transactions on Information Theory
Wireless Dynamics announces first NFC-RFID mini-SD card	Andy Williams	2006-04-05	NFCNews
Yet Another RFID Hack Could Affect Up To 1 Billion Cards		2008-03-14	RFiD Journal
Evaluating Wireless Technologies in Mobile Payments – A Customer Centric Approach	Zmijewska	2005-07	IEEE International Conference on Mobile Business

Samsung additionally identifies and relies on patent or publication references that describe or are otherwise related to the prior art systems identified below, including any patents or publications cited in the claim charts for these systems or elsewhere in these Invalidity Contentions, including Sections V and VI, below. Samsung's investigation into prior art patent and publication references is ongoing, and Samsung reserves the right to identify and rely on additional patent or publication references that are identified through further investigation or discovery. Samsung reserves the right to supplement as further prior art is identified through investigation or discovery.

B. Prior Art Systems and Products

Samsung also contends that the Asserted Claims are invalid based on public knowledge and uses and/or offers for sale or sales of products and services that are prior art under 35 U.S.C. § 102(a) and/or (b); and/or prior inventions made in the United States by other inventors who had not abandoned, suppressed, or concealed them under 35 U.S.C. § 102(g), and that anticipate or render obvious under 35 U.S.C. § 103 the Asserted Claims.

Prior Art	Date of Public Use, Sale, Offer, or Availability	Offering Entity
"Kyocera": the Cellular South / Kyocera / ViVOtech / MasterCard mobile payment technologies and systems and their related phones, software, products, and public U.S. trials, including without limitation the Kyocera's Tempo E2000 handset demonstrated at the CTIA Wireless 2008 trade show in Las Vegas and used as part of the Cellular South WirelessWallet service and trial conducted in 2007, Kyocera ~~E2000~~Jet handsets and ViVOtech software used thereon as part of the Cellular South trial or any other trials, and the MasterCard PayPass used in the Cellular South trial for OTA provisioning of credit cards on Kyocera smartphones.	On or before April 2008	Cellular South, Kyocera Wireless, ViVOtech, MasterCard
"Nokia": Nokia phones with Near Field Communication ("NFC") capabilities, including the Nokia 3220 Series with the Nokia NFC shell used in a 2006 market trial with MasterCard, the Nokia 6131 Series revealed in 2007 at the Consumer Electronics Show (CES), and the Nokia 6212 Classic released in early 2008, as well as the mobile payment technologies and OTA provisioning capabilities provided by Cingular, Visa, Chase, ViVOtech, MasterCard, and others for use with those Nokia phones for mobile payments, including in U.S. mobile payment market trials.	On or before Q3 2008	Cingular, Nokia, Visa, ViVOtech, Chase, MasterCard, Citigroup, 7-Eleven, People's Bank of Paris (Texas), Wells Fargo
"Motorola": Motorola ~~phones with used in~~ mobile payment ~~market trials and the mobile payment~~ technologies and ~~OTA provisioning capabilities provided for use with those phones as part of those market trials.~~systems and their related phones, software, products, and public US trials, demonstrations, and prototypes, including without limitation Motorola Mobile Commerce Platform ("M-Commerce"), the Motorola M-Commerce Applications ("M-Wallet"), the Motorola SLVR NFC Handset Trial Product, and the Motorola [redacted].	On or ~~around February 2007~~before November 7, 2008	Discover, Motorola Mobility, C-Sam, Inc.
PayPal Mobile Payment System	On or before 2007	PayPal
"Fujitsu": Fujitsu and NTT DoCoMo mobile payment technologies and systems and their related phones, software, products, and public U.S. trials, including without limitation the Fujitsu DoCoMo FOMA F900i	On or before August 2008	NTT DoCoMo, Fujitsu

Series handset and other aspects of mobile payment system including but not limited to Osaifu-Keitai and FeliCa, and Edy.		
Handset as configured and used in MasterCard/HSBC trial	On or before January 2007	HSBC, MasterCard, ViVOtech.
Alipay	2004	Alibaba Group
Metavante / Monitise System	2007	Metavante and Monitise Ltd.,
MobileLime	2005	MobileLime (now Catalina Marketing)
Obopay	2007	Obopay
Blaze Mobile Wallet	On or before January 2008	Blaze Mobile
iPhone, Original	June 28, 2007	Apple
iPhone 3G	June 9, 2008	Apple
T-Mobile G1 / HTC Dream	September 2008	HTC, T-Mobile
BlackBerry 8820	September 2007	RIM, AT&T, T-Mobile
"NFC": Near-field communication mobile payment technologies and systems and any NFC-enabled mobile devices, software, products, and public U.S. trials	On or before November 7, 2008	NFC Forum, ISO/IEC, ECMA, Smart Card Alliance, other vendors

Samsung has begun to take discovery of third parties, but the process of identifying and engaging with entities that may have prior art from twenty or more years ago is ongoing. Samsung reserves the right to conduct such discovery and supplement these Invalidity Contentions to include any prior art systems and products that render the asserted claims invalid, if necessary. Samsung may use documentation and publications, physical samples, executable software, or source code as evidence of the relevant functionality of these prior art products or services. Samsung will make available for inspection any physical samples of products, systems, or software listed above, and/or any source code therefor, that it has in its possession or that becomes available during discovery.

V. BACKGROUND: STATE OF THE ART AT TIME OF ALLEGED INVENTION

A. Admitted Prior Art and the Common Specification

The Asserted Patents share a common specification. Citations in this section are to the '411 patent, unless otherwise noted.

As that common specification states, the claimed inventions relate to "systems, devices and/or methods that may be used to provide an adaptive enablement of one or more communications modes based upon having satisfied a proximity criterion. The one or more communications modes may be one or more wireless and/or non-wireless communications modes." 1:5-11. *See also* 1:20-34. An emphasized example is allowing a wireless phone to act as a wallet "only when it is time to pay for an item." 1:25-28.

The specification does not disclose new or improved underlying technological capabilities. It acknowledges that the "adaptivity and mobility aspects of wireless communications" were already "important in people's lives" at the time of alleged invention. 1:15-16. It assumes, in the "Background of the Invention" section, that mobile phones could act as digital wallets. *See* 1:13-27. It does not disclose any new communications protocols and instead acknowledges the existence of NFC, RFID, WiFi, and cellular communications. *See, e.g.*, 7:3-13. Nor does the specification disclose new or improved means of sensing (including physiological/biometric) or proximity detection by mobile phones.

At the heart of the disclosure is a mobile wireless device that "may be configured to enable one or more modes/functions" of itself or of another device "responsive to a proximity criterion having been satisfied." 2:60-3:2. The proximity criterion is a measure of how close the wireless device (or the second device) is to an "entity." 3:3-30. Disclosed examples of entities include people, products for sale, and point of sale terminals (3:31-39), and the entity may or may not be previously known to the wireless device (3:40-51). One of the disclosed proximity detection

methods is detecting a low-power or short range signal radiated from a (third) device that is part of or otherwise associated with the entity. *See* 3:17-21, 40-61.

The specification identifies three "Example/Applications" (4:16 et seq., 5:63 et seq., and 7:63 et seq.) and then discloses various "Other Embodiments" (8:53 et seq.).

"Example/Application No. 1" (4:16-5:62) is directed to using the alleged invention in the context of paying a toll. In this example, the "pay toll" functionality of a user's phone is enabled when the user is proximate to a car that is associated with the user. Then, when the user's phone detects a signal associate with a toll payment point, the "pay toll" functionality operates to pay the toll. A "master/slave" variant of this embodiment is disclosed, wherein the "slave" wireless device associated with a second user senses a signal from the car, responsively requests authorization from the first user's wireless device (the "master"), and enables its own mode after receiving authorization. If that mode is a "pay toll" mode, any transactions made while in that mode may be done using a payment account associated with the user of the "master" wireless device and not the "slave" wireless device.

"Example/Application No. 2" (5:63-7:61) is directed to a wireless device that senses both its location as well as a second parameter related to the device or a user of the device. The device is configured to enable a "first communications mode/function" and/or disable a "second communications mode/function" in response to a proximity evaluation and/or an evaluation of the second parameter. The specification discloses that the "disabling" includes not using or using only infrequently. It also discloses that the proximity and second parameter evaluations may be done repeatedly, with the communications mode/function status maintained or changed accordingly. In this example, the evaluations may also control the sending or receiving of information to or from other devices.

"Example/Application No. 3" (7:63-8:50) is directed to a shopping cart. A user's wireless device establishes connectivity with a shopping cart. The cart senses the items that are added to it, transferring that information to the user's device. The user can pay for the contents of the cart using the wireless device, but perhaps only when the user's device and the cart are both proximate to a point of payment such that one or both can detect a short-range signal associated with the payment point.

The specification then discloses "Other Embodiments," which are just further simple variants on same the theme of sensing a proximity and/or a second parameter and enabling and/or disabling a mode or capability (or making and/or not making a communication) in response. *See* 8:54-12:67.

B. RFID: From the Cold War to Toll Roads

RFID (radio frequency identification technology) was developed as an outgrowth of work with radar during the Second World War. The commonly cited seminal paper is Harry Stockman's "Communication by Means of Reflected Power," Proceedings of the IRE, pp. 1196-1204, October 1948. A famous early user of the technology was Leon Thermin, inventor of the idiosyncratic electronic musical instrument that bears his name. He used RFID in the "Great Seal Bug" or "The Thing," which allowed the Soviets to eavesdrop on the US embassy in Moscow throughout the late 1940s. *See* https://people.ece.uw.edu/nikitin_pavel/papers/RFID-vox_2013.pdf; *see also* https://en.wikipedia.org/wiki/The_Thing_(listening_device).

In the 1960s, companies such as Sensormatic (https://www.sensormatic.com/about-us) and Checkpoint Systems (https://checkpointsystems.com/rfid-solutions/) were founded to commercialize RFID tag users for asset tracking. In the 1970s, the Port Authority of New York and New Jersey tested systems for electronic toll collection, including those built by General

Electric and Westinghouse. *See* https://transcore.com/wp-content/uploads/2017/01/History-of-RFID-White-Paper.pdf.

In 1973, U.S. Patent No. 3,713,148 issued on a 1970 application for an RFID tag with rewritable memory. That same year, U.S. Patent No. 3,752,960 issued on a 1971 application for an RFID tag that could unlock a door when a reader associated with the door recognized the data transmitted from the RFID transponder. Lock maker Schlange licensed that patent. *See* https://venturebeat.com/business/charlie-walton-inventor-of-rfid-passes-away-at-89/; https://www.rfidjournal.com/expert-views/the-history-of-rfid-technology/76202/.

In the 1980s, RFID for toll collection rolled-out commercially, most famously with the launch of E-ZPass across multiple states and transit authorities in 1993. *See* https://roadpricing.blogspot.com/2011/09/history-of-ez-pass.html; https://www.nytimes.com/2001/09/09/nyregion/call-it-e-zpass-the-hard-way.html.

In the 1990s and 2000s, RFID for contactless payments took center stage. For example, in 1997, petrochemical company Mobil deployed Speedpass, a contactless payment system, that originally used a keychain fob with an embedded RFID radio transponder. *The Mobil Speedpass and Mobile Commerce*, Rottenberg and Liu, MIT Undergraduate Research Journal, Vol. 7, Fall 2002. When proximate to a fuel pump or checkout counter, the transponder would activate and communicate with the merchant system to charge purchases to a credit card or check/debit card that the customer designated when they enrolled or authorized the device. *See* https://web.archive.org/web/20040605210151/http://www.exxonmobil.com/Corporate/Newsroom/Newsreleases/Corp_xom_nr_311000_2.asp.

The Speedpass fob could also be used for payments at certain McDonald's restaurants and Stop & Shop grocery stores. *See, e.g.*, Rottenberg,

https://usatoday30.usatoday.com/tech/news/2001-05-29-mcdonalds-e-payments.htm; https://web.archive.org/web/20040703120640/http://www.speedpass.com/how/index.jsp; https://www.nbcnews.com/id/wbna3072638; https://abcnews.go.com/Business/story?id=87928. By October 2000, more than four million U.S. customers were using Speedpass. Rottenberg, http://www.exxonmobil.com/Corporate/Newsroom/Newsreleases/Corp_xom_nr_311000_2.asp. In 2002, even Timex wristwatches were enabled for Speedpass. https://web.archive.org/web/20040623074724/http://www.speedpass.com/news/article.jsp?id=51

.

A similar program was FreedomPay, launched in the early 2000s to support contactless payment. Customers could use a contactless fob or payment card at checkout, adding funds to the card over the internet, via phone, or even at the time of payment. *See, e.g.*, https://web.archive.org/web/20070707222446/https://www.freedompay.com/AboutFreedomPay/default.aspx; https://www.secureidnews.com/news-item/freedompay-makes-waves-in-contactless-payment/; https://usatoday30.usatoday.com/tech/news/2001-05-29-mcdonalds-e-payments.htm.

C. NFC Is Standardized in the 1990s and early 2000s.

By the early 1990s, there was a international and cross-industry focus on using RFID in smartcards and other devices that could exchange data when proximate to each other. The ISO released the ISO-14443 standard for such devices in 1995. *See, e.g.*, https://www.rfidlabel.com/beginners-guide-comprehensive-analysis-of-iso-14443-protocol/:

> The origin of the ISO-14443 protocol can be traced back to the early 1990s. With the rise of contactless card technology, the demand for convenient and secure short-range wireless communication is increasing. Traditional contact smart cards require physical contact, which is inconvenient and prone to wear and tear in many application scenarios. Therefore, contactless technology is gradually gaining attention.
>
> Against this backdrop, the International Organization for Standardization (ISO) set out to develop a standardized contactless communication protocol. It ensures interoperability between cards and readers from different vendors. This standardization effort led to the creation of the ISO0-14443 protocol.
>
> **Phase I: Initial version of ISO-14443 (1995)**
>
> In 1995, the initial version of the ISO-14443 standard was released. The initial version included the basic framework of the protocol, covering the physical characteristics and communication requirements of contactless cards.
>
> The goal of the standard was to provide technical specifications for short-range communication (typically within 10 centimeters) between contactless smart cards and readers.
>
> In the initial version, the protocol focuses primarily on RF communications at 13.56 MHz. A frequency band commonly used for short-range RFID applications.

In 2002, Philips and Sony announced their intent to cooperatively develop the NFC standard, which built atop ISO 14443. https://www.securetechalliance.org/philips-and-sony-announce-strategic-cooperation-to-define-next-generation-near-field-radio-frequency-communications/. The two companies proclaimed that "Wireless NFC technology will operate on 13.56 MHz and allow for the transfer of any kind of data between NFC enabled devices such as mobile phones, digital cameras and PDA's as well as to PC's, laptops, game consoles or PC Peripherals, across a distance of up to twenty centimeters and aiming at speeds fast enough to transfer high quality images. At communication speed up to 212 kbit/s the NFC technology is fully

compliant to both Philips' existing Mifare™ and Sony's FeliCa™ contactless smartcard technologies." *Id*.

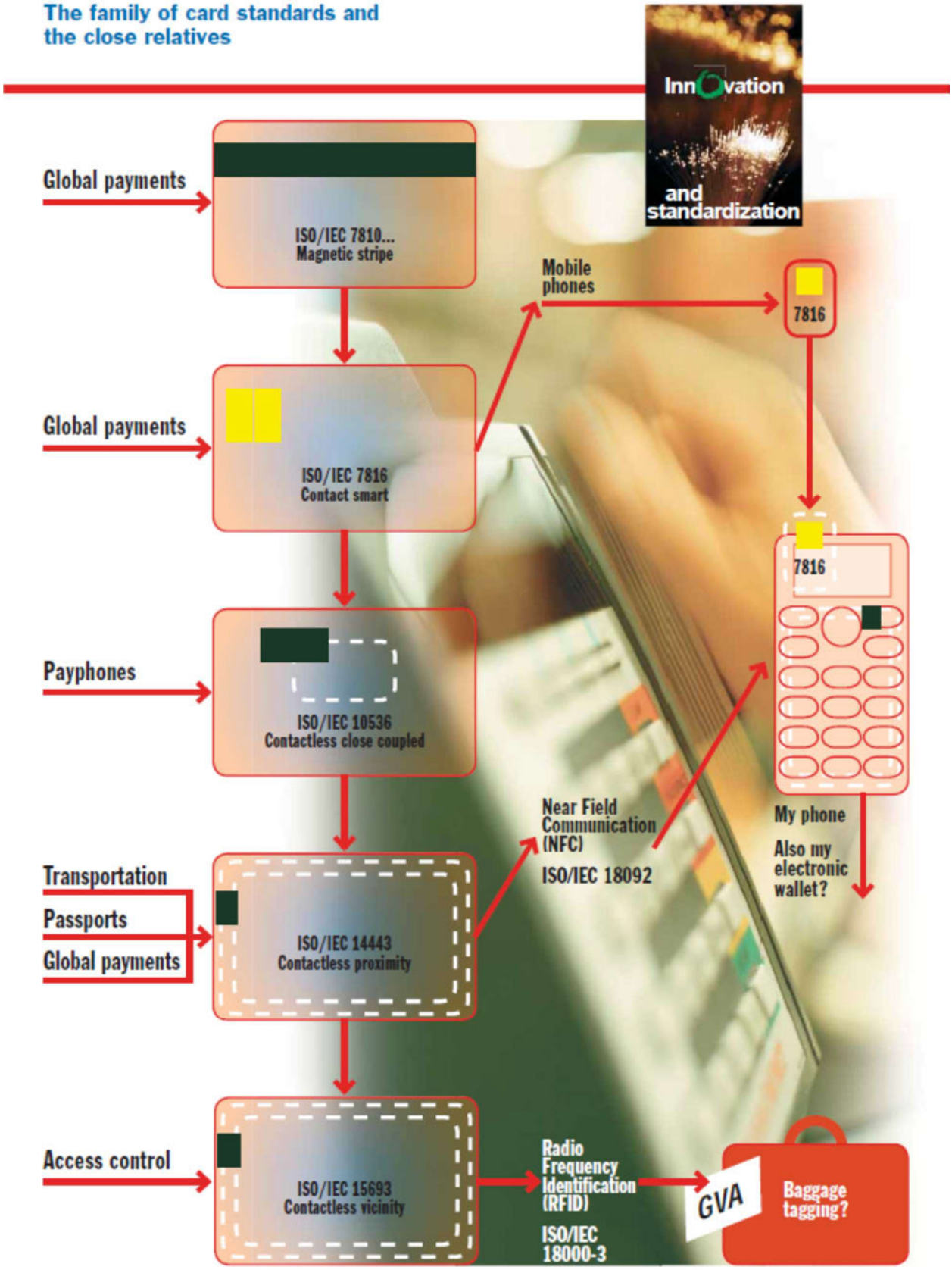
Among the announced goals was "to build a ubiquitous open infrastructure of NFC-compliant devices which effectively incorporate smart-key and smartcard reader functions, providing a convenient communication method for services such as payment (including credit card), ticketing, and accessing online entertainment content (e.g. gaming) through the devices." *Id*. ISO 18092 was released just a year later, in 2003. ISO 18092 provided a more complete overall framework for two devices to communicate via RFID. *See, e.g.*, "Near Field Communication in the Real World, Part 1" by Innovision Research & Technology. ("Innovision 2006 White Paper"); https://www.sony.net/Products/felica/NFC/ ("Sony NFC"); https://www.rfidlabel.com/beginners-guide-comprehensive-analysis-of-iso-14443-protocol; https://e2e.ti.com/cfs-file/__key/telligent-evolution-components-attachments/00-667-01-00-00-30-14-15/ISO14443-Overview_2D00_v5.ppt.

The Innovision 2006 White Paper describes NFC at pages 4-6:

> NFC is a short-range, standards-based wireless connectivity technology, based on RFID technology that uses magnetic field induction to enable communication between electronic devices in close proximity. It provides a seamless medium for the identification protocols that validate secure data transfer. This enables users to perform intuitive, safe, contactless transactions, access digital content and connect electronic devices simply by touching or bringing devices into close proximity.
>
> NFC operates in the standard unlicensed 13.56MHz frequency band over a distance of up to around 20 centimetres. … For two devices to communicate using NFC, one device must have an NFC reader/writer and one must have an NFC tag. The tag is essentially an integrated circuit containing data, connected to an antenna, that can be read and written by the reader.
>
> There are two modes of operation covered by the NFC protocol: active and passive. In active mode, both devices generate their own radio field to transmit data. In passive mode, only one device generates a radio field, while the other uses load modulation to transfer data. … The passive mode of communication is very important for battery-powered devices like mobile phones and PDAs that need to prioritize energy use. The

> NFC protocol enables such devices to be used in power-saving mode, so that energy can be conserved for other operations.
>
> …
>
> The underlying layers of NFC technology are ISO, ECMA and ETSI standards. Because NFC is compliant with the main international standard for smartcard interoperability, ISO 14443, it is compatible with the millions of contactless smartcards and readers already in use worldwide.

By February 2006, ISO Focus, the official ISO magazine, published an issue with several articles related to RFID, NFC, and biometrics. ISO Focus Vol. 3, No. 2, Feb. 2006 (ISO Focus 2006). The articles included "RFID – A technology whose time has come!" (pp. 20-22), "Revamping the supply chain with RFID" (pp. 23-26), "Biometrics – Rising to the challenge of technology innovation" (pp. 28-33) and "Cards for all seasons" (pp. 33-37). The latter of those specifically discussed contactless payment using RFID. The issue included this figure, at page 35, illustrating the integration of mobile phones and ISO standards for contactless payment.


The family of card standards and the close relatives
Innovation and standardization
Global payments
ISO/IEC 7810... Magnetic stripe
Mobile phones
7816
Global payments
ISO/IEC 7816 Contact smart
7816
Payphones
ISO/IEC 10536 Contactless close coupled
Near Field Communication (NFC)
ISO/IEC 18092
My phone
Also my electronic wallet?
Transportation
Passports
Global payments
ISO/IEC 14443 Contactless proximity
Access control
ISO/IEC 15693 Contactless vicinity
Radio Frequency Identification (RFID)
ISO/IEC 18000-3
GVA
Baggage tagging?

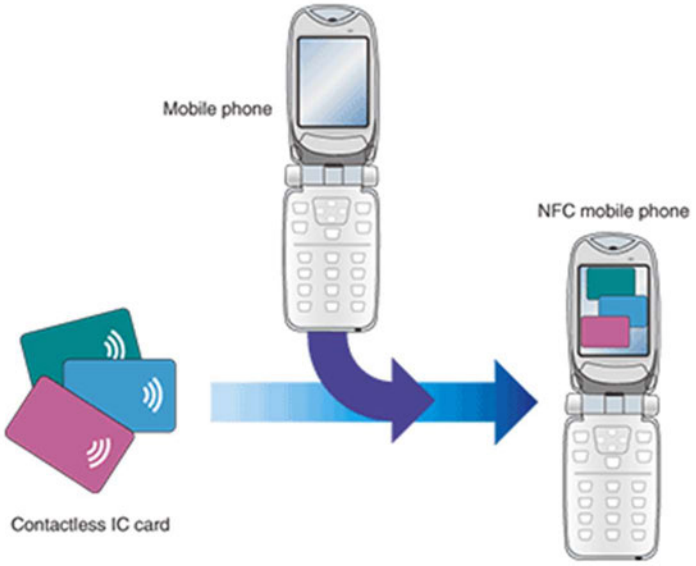
In 2004, a year after the release of the ISO NFC standard, Nokia, Philips, and Sony formed the NFC Forum, www.nfc-forum.org. *See* https://www.ntt-review.jp/archive/ntttechnical.php?contents=ntr200905gls.html (Nakamura 2009); Innovision 2006 White Paper; Sony NFC. One of the goals of the NFC Forum was to promulgate interoperability standards or specifications and encourage the development of compliant products. As early as 2006 it was touting real-world NFC successes, including mobile phone proximity payment successes in Atlanta, Georgia as well as in Japan and France. *See* Near Field Communication and the NFC Forum: The Keys to Truly Interoperable Communications. By 2007, members included the world's leading operators of mobile phone networks, makers of mobile phones, and leaders in related industries such as semiconductors and consumer electronics. Nakamura 2009.

As the Innovision 2006 White Paper explained on page 6:

> In June 2006, the NFC Forum introduced standardized technology architecture, initial specifications and tag formats for NFC-compliant devices. … In addition, the NFC Forum announced the initial set of four tag formats that all NFC Forum-compliant devices must support. These are based on ISO 14443 Types A and B (the international standards for contactless smartcards) and FeliCa (derived from the ISO 18092, passive communication mode, standard). Tags compatible with these mandatory formats are available initially from Innovision, Philips, Sony and other vendors, and more than one billion tags are already deployed globally.
>
> The NFC Forum chose the initial tag formats to cater for the broadest possible range of applications and device capabilities.

A focus of the NFC Forum was integration of mobile phones into the contactless payment ecosystem. As documented in an NFC Forum October 2008 whitepaper "Essentials for Successful NFC Mobile Ecosystems" (described and excerpted in Nakamura 2009), the NFC-Forum's mobile task force acknowledged that systems based on the FeliCa and MiFare systems (discussed elsewhere herein) were de facto standards. *Id*. The NFC Forum leveraged these commercial

deployments in its proposed standard architecture for an "NFC mobile phone," as pictured below. *Id*.

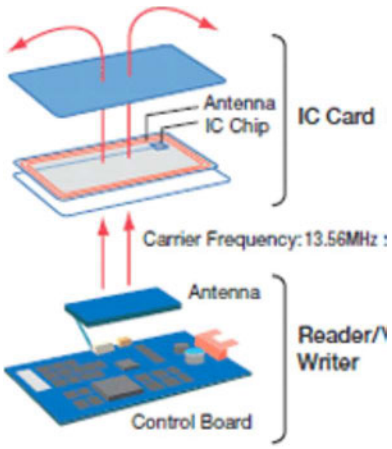


Another group documenting the use of NFC and mobile devices for contactless payments – and advocating for increased adoption – was the Smart Card Alliance (now known as the Secure Technology Alliance). See https://www.securetechalliance.org/.

D. Transactions with Contactless Smartcards

1. Sony's FeliCa Contactless Smartcard

Sony developed its own RFID smartcard, FeliCa, in 1989, and a commercial implementation called "Octopus" deployed in Hong Kong in 1997. https://www.sony.net/Products/felica/casestudy. A FeliCa-enabled payment card was a standard card with an RFID antenna and integrated circuit (IC) chip:



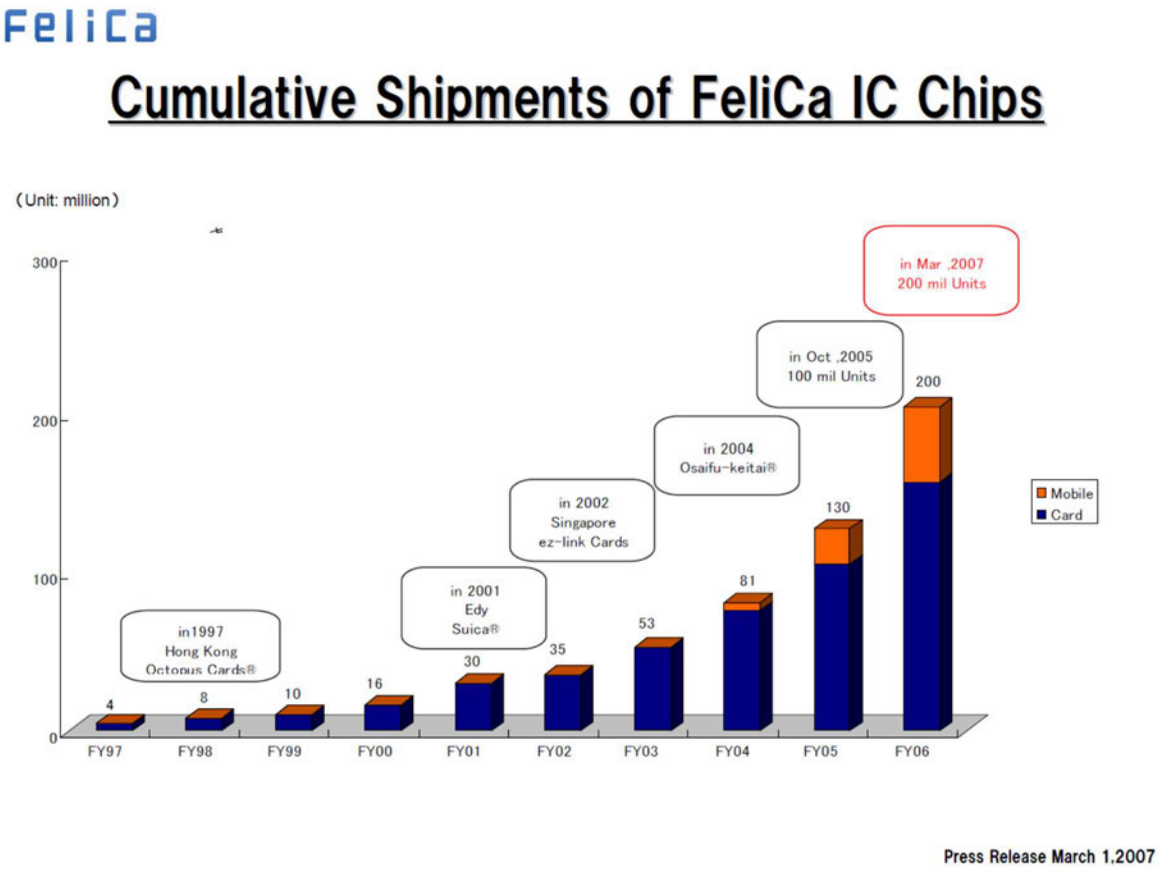
IC card and Reader/Writer

https://web.archive.org/web/20081002044830/http://www.sony.net/Products/felica/abt/dvs.html

Like ISO 14443 compliant implementations, a FeliCa smartcard communicated with a FeliCa reader/writer on the 13.56 MHz carrier frequency. *Id.*

As illustrated in a video available from Sony, one of the many uses of FeliCA cards was in contactless bankcards. *See* https://web.archive.org/web/20061123111124/http://www.sony.net/Products/felica/mov/data/itd_FeliCa.wmv; *see also* https://www.sony.com/en/SonyInfo/News/Press/200012/00-1225E/ (a 2000 announcement of what became the EDY payment card, which used FeliCa).

FeliCa rapidly gained popularity throughout parts of Asia and especially in Japan, where the smartcards were used for a multitude of purposes, including transactions. By March 2007, Sony had shipped over 200 million FeliCa chips, a sizable number for use in mobile phones.



https://www.sony.com/en/SonyInfo/News/Press/200703/07-021E/.

2. Philips/NXP MIFARE contactless smart cards

Meanwhile, in 1994 Philips Semiconductors, which soon became NXP Semiconductors, commercially launched the first MIFARE contactless smart cards. *See* https://nexqo.com/2023/12/mifare-cards-guide/. MIFARE cards were put to similar uses as FeliCa cards. *See* https://www.nxp.com/company/about-nxp/smarter-world-blog/BL-25-YEARS-OF-MIFARE; https://www.sciencedirect.com/science/article/abs/pii/S1363412710000348 (Mayes, K. E., & Cid, C. (2010). The MIFARE Classic story, Information Security Technical Report, 15(1), 8 – 12. https://doi.org/10.1016/j.istr.2010.10.009), https://nexqo.com/2023/12/mifare-cards-guide/. It was estimated that by March 2008 there were over one billion MIFARE chips in use around the world, mostly in smartcards. https://www.rfidjournal.com/news/yet-another-rfid-hack-could-affect-up-to-1-billion-cards/83155/.

E. Mobile Phones and Wireless Connectivity

1. Wireless mobile phones have been in use since the 1940s.

Developments in contactless smartcards coincided with surging popularity of mobile phones and smartphones.

The first mobile phones, launched in the 1940s, were vehicle based and used a single system, like AT&T's Mobile Telephone Service. "The Cell-Phone Revolution," American Heritage of Invention & Technology, August 22, 2007. ("Farley," available at https://www.americanheritage.com/content/cell-phone-revolution). See also https://techbuzz.att.com/explainers/history-of-the-mobile-phone-from-1g-to-5g/ ("From 1G to 5G"). Cellular service was described and known at least as early as 1947, and AT&T immediately began making plans to deploy it for mobile phones. Farley. With enabling technological advances in electronic componentry and with appropriate regulatory approvals, mobile phones that used

cellular communications launched in the late 1960s – including one used by President Nixon on a train between New York City and Washington, D.C. Farley.

The first hand-held cell phone that was available to the general public was used in April 1973. McNamee, "50 years ago, Martin Cooper made the first cellphone call," at 1 (2023). See also, Farley. The very first smartphone, the Simon Personal Communicator (SPC), was released by IBM in 1994. Tocci, "Smartphone History and Evolution," at 1 (2023). The SPC had the ability to send and receive emails and faxes, and also had a calendar, address book, and a native appointment scheduler. *Id*. Less than fifteen years later, before the priority date of the Asserted Claims the iPhone (June 29, 2007) and the Android-powered T-Mobile G1 smartphone (September 23, 2008) were released. See https://www.apple.com/newsroom/2007/06/28iPhone-Premieres-This-Friday-Night-at-Apple-Retail-Stores/ and https://www.t-mobile.com/news/press/t-mobile-unveils-the-t-mobile-g1-the-first-phone-powered-by.

2. Mobile phones wireless technologies were well established.

In the 1990s, mobile phones used could operate on two different types of "2G" digital cellular networks, GSM or CDMA See https://www.redorbit.com/reference/the-history-of-mobile-phone-technology ("Red Orbit History"). See also https://1nce.com/en-us/resources/news/blog/cellular-mobile-standards ("1NCE"). The Nokia 3210, which sold over 160 million units, operated on 2G networks. See https://www.cengn.ca/information-centre/innovation/timeline-from-1g-to-5g-a-brief-history-on-cell-phones/ ("Cengen").

To support faster data transfers and generally improve upon the 2G experience, carriers launched packet-switched "3G" networks in the early 2000s, starting with NTT DoCoMo in Japan in 2001. *See* Red Orbit History.

By the end of the 2000s, network operators and mobile phone manufacturers had begun implementing 4G networks. *See* Red Orbit History.

In parallel with the development of improved cellular services, the industry also standardized wireless versions of local area networks. The first IEEE standard for Wi-Fi (802.11) was published in 1997, and it used the unlicensed 2.4 GHz spectrum. See https://standards.ieee.org/beyond-standards/the-evolution-of-wi-fi-technology-and-standards ("Evolution of Wi-Fi"). The 802.11a standard was published in 1999. *Id*.

Around the same time, Bluetooth began to be widely adopted. Early work by Ericsson and others was standardized as IEEE 802.15.1 in 2002 (Bluetooth 1.1). See https://www.mokosmart.com/guide-on-different-bluetooth-versions/. Bluetooth 2.0, released in 2004, was full-duplex. *Id*. By 2007, Bluetooth 2.1 devices could exchange handshake information and connect via NFC. See http://blue-tooth.50webs.com/bluetooth_2.1.html.

Some of these technologies use OFDM (orthogonal frequency division multiplexing) or OFDMA (a multiple access or multiple user protocol based on OFDM), which are referenced in the common specification. OFDM dates back to work in 1966 at Bell Labs, and can trace its origins to work patented in 1942 by Hedy Kiesler Markey, better known as Hedy Lamarr. See The History of Orthogonal Frequency-Division Multiplexing, IEEE Communications, Vol. 47, Issue 11, November 2009. *See also* U.S. Patent No. 3,488,445 ("Orthogonal Frequency Multiplex Data Transmission System"). OFDMA was widely discussed at least by 1996. See https://ieeexplore.ieee.org/document/5483464 ("A Review of OFDMA and Single-Carrier FDMA" Cochina and Sari, 2010).

The 1999 WiFi standard (IEEE 802.11a) used OFDM. *See* Cochina and Sari, *see also* https://www.tek.com/en/documents/primer/wi-fi-overview-80211-physical-layer-and-transmitter-measurements. So too did parts of the IEEE 802.16 wireless WiMA standard adopted in 2004 and 2005. *See* Cochina and Sara; *see also,* 802.16 OFDM Overview at

https://helpfiles.keysight.com/csg/89600B/Webhelp/Subsystems/80216ofdm/content/wimax_overview.htm; OFDM Basics at https://helpfiles.keysight.com/csg/n7615/Content/Main/OFDM_Basics.htm.

By 2008, it was also known that OFDMA would be part of the 3GPP LTE standard ("4G"). *See* Cochina and Sara. *See also, e.g.*, Multi-Carrier and Spread Spectrum Systems: From OFDM and MC-CDMA to LTE and WiMAX, 2nd Edition, Fazel and Kaiser, Wiley Nov. 3, 2008. See also documents available at https://www.3gpp.org/specifications-technologies/releases/release-8 (showing that versions of Release 8 of the LTE 4G standard were published as early as March 2008 before being finalized in December 2008; also illustrating the breadth of the community involved in preparing and evaluating the proposal). *See also* Performance Analysis Of OFDM (Ahamed).

Time division duplexing (TDD) is a long-known technique for emulating full-duplex communication over a half-duplex link, whereby use of the link (a given frequency) is allocated by time, with one device allowed to send communication during one period, and the other device allowed to send during the next period. *See, e.g.*, https://www.everythingrf.com/community/what-is-lte-tdd. Both Wi-Fi and Bluetooth use TDD (*see* https://www.teracomtraining.com/tutorials/teracom-tutorial-wireless-LANs-WiFi-802.11.htm). RFID implementations, including those with passive tags, may also use TDD. *See* https://www.eetimes.com/rfid-technology-and-testing/.

3. Mobile phones incorporated multiple wireless technologies.

Most mobile phones at the time of alleged invention connected to a 2G or 3G network (or a variant thereof). And it was common for those phones to also support wireless technology that let them connect nearby device over shorter range protocols. *See, e.g.*, https://www.gsmarena.com/mobile_phones_evolution_features-review-501p3.php (documenting

the popularity of smartphones with Bluetooth and IrDA capabilities as measured by searches for those models on a popular website) and https://www.gsmarena.com/mobile_phones_evolution_features-review-501p2.php (doing the same for smartphones with 802.11 WiFi capabilities). Indeed, this is acknowledged in the "Background of the Invention" section of the specification, which acknowledges that mobile phones that could communicate using a variety of wireless protocols and frequencies were well known at the time of alleged invention. '411 patent at 1:15-61.

For example, 1998's Nokia 6150 supported GSM cellular connectivity at 900 MHz and 1800-1900 MHz as well as IrDA (Infrared Direct Access). *See* https://www.gsmarena.com/nokia_6150-10.php; https://en.wikipedia.org/wiki/Nokia_6150; https://www.wsj.com/articles/SB102641837585513440.

The Ericsson R520 (2000) and T39 (2001) may have been the first and second commercially released mass-market smartphones with Bluetooth connectivity. *See* https://lpcwiki.miraheze.org/wiki/Ericsson_T39; https://www.gsmarena.com/ericsson_t39-252.php; https://www.mobilephonemuseum.com/phone-detail/r520m, https://www.gsmarena.com/ericsson_r520m-199.php. Both also used GSM at the 900 and 1800-1900 MHz ranges, could use the GPRS data protocol, and supported the 1.0b version of Bluetooth. *Id*.

Nokia released its first Bluetooth-enabled phone, the 6310, around the same time. *See* https://en.wikipedia.org/wiki/Nokia_6310; https://www.gsmarena.com/nokia_6310-240.php; https://www.mobile-review.com/review/nokia-6310-en.shtml (noting 10 meter Bluetooth range). In addition to supporting Bluetooth 1.1, it supported GSM for cellular connectivity and included IrDA connectivity.

In 2006, Calypso demonstrated a dual-mode smartphone that supported both GSM and WiFi. *See* https://www.globenewswire.com/news-release/2006/02/27/339928/2817/en/Calypso-Wireless-Successfully-Demonstrated-the-C1250i-Wi-Fi-GSM-VoIP-Skype-Call-Connectivity-Cellular-Phones-on-Vodafone-Network-at-3GSM-Congress.html; https://www.geekzone.co.nz/content.asp?contentid=4493.

In 2005, Samsung released the SCH-i730 smartphone, which featured Wi-Fi, Bluetooth, IrDA, **and** CMDA connectivity. *See* https://www.cnet.com/reviews/samsung-sch-i730-verizon-wireless-review/; https://www.phonescoop.com/phones/phone.php?p=667.

The BlackBerry 8820, released in March 2008, included Bluetooth, Wi-Fi, and GSM support. *See* https://www.phonescoop.com/phones/phone.php?p=1280, https://www.t-mobile.com/news/press/t-mobile-usa-launches-blackberry-8820; https://www.cnet.com/reviews/blackberry-8820-t-mobile-blackberry8820tmb-review/.

Numerous phones supported RFID and NFC in addition to cellular and other connectivity, as discussed below. And if users had phones or other wireless devices that did not support NFC "out of the box," they could add the necessary hardware. For example, in 2006 Wireless Dynamics released the SDiD 2010, which integrated NFC and smart card functions into devices with mini-SD expansion slots. https://www.secureidnews.com/news-item/wireless-dynamics-announces-first-nfc-rfid-mini-sd-card/. This was a follow-up to the 2005 release of a similar device that worked in SD expansion slots. https://www.secureidnews.com/news-item/sd-rfid-card/. According to the announcement, "[t]he SDiD 2010 is also integrated with the SAM (Secured

Access Module) used for many contactless payment standards. Now Smartphones, cell phones and PDA's with externally accessible mini-SD connectors can be enabled by the SDiD 2010 for mobile payment, e-ticket, retail and other NFC applications. Consumers can use their mini-SDiD enabled phone to make contactless payments, redeem coupons, instant rewards and contactless transactions quicker, easier and secure." *Id*. "The SDiD 2010 supports reading and writing of ISO14443A, Philips MIFARE and Philips MIFARE DESFire contactless tags and labels. In addition, the SDiD 2010 is capable of peer to peer communications utilizing NFCIP-1 and ISO 18092 standards. With the embedded SmartMX SAM processor, the SDiD 2010 can be loaded with certified contactless payment applications and used as credit, debit and stored-value payment cards. The SDiD 2010 operates at 13.56MHz and supports a wide range of Smartphones and PDAs with Microsoft Pocket PC 2002/2003, Windows Mobile 2003, Windows Mobile 5.0, and Palm OS 4.1 and up operating systems." *Id*.

F. Use of Mobile Phones in Contactless Payment Systems

1. GSM Association's Pay-Buy-Mobile

In February 2007, the GSM Association (a global trade organization for mobile phone operators) announced its "Pay-Buy-Mobile" initiative. https://en.prnasia.com/releases/global/GSM_Association_Aims_for_Global_Point_of_Sale_Purchases_by_Mobile_Phone-1477.shtml. With the initial support of fourteen operators having a total of over 900 million customers, the plan was set to begin with a business model analysis followed by an end-to-end trial in Korea later in 2007. *Id*.; *see also* https://www.rcrwireless.com/20070425/archived-articles/pay-buy-mobile-initiative-gets-underway-with-major-backing; https://web.archive.org/web/20070828063004/http://www.gsmworld.com/news/press_2007/press07_33.shtml.

2. Kansas City Federal Reserve Bank Publications

In the United States, institutions like the Federal Reserve Bank of Kansas City were studying the impact of contactless payments and considered the use of phones in that context. In a 2004 briefing on payment types at point of sale, the Kansas City Federal Reserve noted that "contactless devices" and "biometric devices" were emerging as POS payments mechanisms in the United States. Terri Bradford, 2004. "Payment types at the point of sale : merchant considerations," Payments System Research Briefing, Federal Reserve Bank of Kansas City, issue Dec. The article noted that "RFID payment technology can be housed in cards, watches, key fobs, and even cell phones. The payment portion of an RFID transaction typically relies on existing credit and debit card infrastructures." *Id*. at 4. With respect to biometrics, it recited that "[b]iometrics identifies a person based on physical characteristics, such as a fingerprint, iris, face, voice, or handwriting. This technology is being employed now in payment devices that are being used by a few merchants, primarily grocery stores. By having a consumer place his or her finger on a fingerprint-reading device, the merchant can confirm the consumer's identity, and the selected form of payment—credit or debit card—can be accessed and used." *Id*.

A 2005 article focused on contactless payment systems, characterizing them as "'traditional' payments (credit and debit cards, for the most part) that utilize microchips and radio frequency identification or near field communication technologies to effect transactions without physical contact between the payment device and the point of sale (POS) terminal." Terri Bradford, 2005. "Contactless: the next payment wave?," Payments System Research Briefing, Federal Reserve Bank of Kansas City, issue Dec. The article noted that "the contactless element" could be included in "key fobs, watches, or even telephones." *Id*. at 2.

After describing the SpeedPass system discussed herein, it also mentioned offering from American Express, Mastercard, and Visa: "In 2003, American Express launched its ExpressPay

'waveable' product, and MasterCard introduced PayPass, a 'tap and go' product. And, in 2004, Visa introduced VisaWave. Whether waved or tapped, all employ a standard, open technology and can be used for payment at any merchant that is able to accept it." *Id*. at 2. It went on to describe how card issuers had announced plans to issued millions of credit and debit cards that worked with these systems. *Id*.

By 2006, it recognized the increasing use of phones in that context. "And, contactless payments also are on the rise. Where consumers have been exposed to contactless payment methods, such as Speedpass at Exxon-Mobil gas stations and PayPass and blink at CVS pharmacies, they reportedly have liked them and would use them more often if they were more widely available. Mobile phone technologies provide another platform to enable all of these types of activities.." Terri Bradford, 2006. "Paper, plastic... or phone?," Payments System Research Briefing, Federal Reserve Bank of Kansas City, issue Dec. That article noted that "Several technologies are available for mobile-phone payment and banking. These include near field communication (NFC), short message service (SMS), and wireless application protocol (WAP) technologies. In addition, payments-related applications can be downloaded to reside directly on the mobile device." *Id*. at 2. Regarding those applications, the article observed that users "essentially 'register' their device for use by entering the phone number and creating a PIN." *Id*. The article also documented several of the NFC trials discussed elsewhere, including the Chase/Visa/Cingular trial in Atlanta. It concluded with an observation that "as it relates to payment acceptance, NFC-based mobile payments may experience growth related to payment terminals already deployed for use with contactless payment cards." *Id*. at 4.

In a September 2007 presentation, the author of that article commented that proximity mobile payments "facilitated by NFC technology" presented "a complex landscape." Terri

Bradford, *Paper, Plastic, or Phone…* (Sept. 27, 2007), *available at* https://www.kansascityfed.org/Speeches/documents/2371/speeches-Bradford_FSTC9-27-07.pdf). This was illustrated by a slide showing some of the credit card companies, issuers, mobile phone providers, mobile network operators, retailers, technology enablers, and others involved in that landscape, and concluded with a reference to publications from the Smart Card Alliance.

In a September 2007 article, the Federal Reserve Bank of Kansas City reported on mobile payments in the Japan, South Korea, and the United States. Bradford & Hayashi, 2007. "Complex landscapes: mobile payments in Japan, South Korea, and the United States," Payments System Research Briefing, Federal Reserve Bank of Kansas City, issue Sep. The article recounted that in Japan, "mobile 'proximity' payments (that is, at point of sale) using contactless integrated circuit (IC) chips has become most prevalent. In July 2004, NTT DoCoMo, the largest mobile phone operator in Japan, began deploying mobile devices containing the FeliCa contactless IC chip

developed by Sony. The FeliCa chip makes it possible for mobile devices to contain multiple forms of data including … bank account numbers and balances, credit account information… and more. As a result, … NTT DoCoMo phones enabled consumers to use their devices as a substitute for cash and cards at vending machines and merchants' points of sale." *Id*. It then described various mobile proximity payment platforms that leveraged this infrastructure, including for credit card payments. *Id*. at 2.

It went on to describe that in South Korea, early mobile payment platforms were based on infrared connectivity. *Id*. at 2. Then, in 2003, a South Korean bank launched BankOn, which used IC chips. *Id*. It reviewed how multiple IC options existed in South Korea, including Visa PayWave and MasterCard PayPass solutions. *Id*. As of 2007, at least one mobile phone operator allowed customers to download cred card applications over the air onto secure SIM cards, which could then be used for contactless payments at points of sale. *Id*. at 3.

Finally, the article turned to the United States. It noted that tempering "strong interest" was "the sheer number of financial institutions, the myriad card networks, mobile network operators, hardware and software providers, and other stakeholders results in a host of challenges and considerations." *Id*. It pointed out that nevertheless, numerous pilots were underway (including those referenced herein). It pointed to the rise of mobile banking (managing accounts and paying bills, but not point of sale transactions) as a further impetus for mobile payments in the United States. *Id*. The rise of contactless payment cards was also said to "no doubt pave the way for mobile proximity payments." *Id*. at 4.

3. In Japan, NTT DoCoMo's Osaifu-Keitai Built on FeliCa

Japanese companies had been filing patents related to mobile phone proximity payments since at least 2000. *See, e.g.*, JP2001-273451 (Aoki) (disclosing a phone with a high power cellular

communication service and a lower power service, like Bluetooth, used for transactional communications).

In light of the ubiquity of FeliCa smartcards and the growing popularity of smartphones, in 2004 NTT DoCoMo introduced Osaifu-Keitai ("Wallet Mobile"). This launch, just a year after the ISO NFC standard was released, reflected that necessary technical solutions were well-understood and affordable enough to be in mass produced consumer phones – what they needed was viable commercial models, not further technical developments. Osaifu-Keitai was comprehensively covered in the English language and followed by relevant audiences in the United States. *See, e.g.*, early 2006 English-language material from NTT DoCoMo at https://web.archive.org/web/20060813065056/http://www.nttdocomo.co.jp/english/service/imode/osaifu/index.html ("DoCoMo Osaifu-Keitai Page"), and U.S. media coverage at, e.g., https://www.infoworld.com/article/2332829/only-in-japan-the-best-technologies-you-can-t-buy-2.html ("Only in Japan"), https://www.nbcnews.com/id/wbna5225043 ("New phones could replace wallets") and https://fareastgizmos.com/mobile_phones/osaifukeitai_docomos_powerfully_convenient_mobile_wallet.php ("Far East Gizmos").

As explained above, the FeliCa infrastructure was already in place, meaning many retailers and vendors in Japan already had terminals or payment systems users could use for contactless payment via fobs or smartcards. This type of implementation is documented in a 2003 white paper from the Smart Card Alliance. "Contactless Payment and the Retail Point of Sale: Applications, Technologies and Transaction Models", Smart Card Alliance, March 2003 ("SCA 2003 Whitepaper"). For example, at pages 7 and 8 it describes the FeliCa-based Octopus system deployed in Hong Kong, where "[t]welve Hong Kong banks and one credit card company support

the automatic add-value service" and customers can pay at "more than 160 merchants." In Hong Kong Nokia released "a cover for one of their mobile phones that includes an embedded Octopus chip and antenna, enabling commuters to sue their phone to make Octopus payments." *Id*.

As described by NTT DoCoMo, Osaifu-Keitai was a service for "mobile phones equipped with contactless IC card, as well as its useful function/services enabled by the IC card. With this function, mobile phones can be utilized as electronic money, credit card, electronic ticket, membership card, airline ticket, and more." DoCoMo Osaifu-Keitai Page at "What's Osaifu-Keitai":

What's "Osaifu-Keitai"?

"Osaifu-Keitai" refers to mobile phones equipped with contactless IC card, as well as its useful function/services enabled by the IC card. With this function, mobile phones can be utilized as electronic money, credit card, electronic ticket, membership card, airline ticket, and more.

Let one "Osaifu-Keitai" replace your wallet and all the other things in your pocket

The functions of items you've kept in your wallet until now - such as money and various cards - can all be combined and carried with you in one phone.

More useful than your wallet

You can place the functions of bills and coins as well as point cards, tickets, etc. in your mobile phone and carry them with you all the time.

More useful than regular cards

You can check the credit balance, point totals, and purchase history on the mobile phone screen, and use the i-mode network to add e-money credit, download tickets, or pay for products and services.

Plus...

There is also discount bonus points and other special privileges exclusively for "Osaifu-Keitai".

"Osaifu-Keitai": Just try it

For example, pre-installed "Edy" e-money

1 Activate the "Edy" i-appli and select Edyチャージ (Edy credit) from the 主なメニュー (Main Menu).

2 On the charging screen, enter your password and the e-money amount you want to add.

3 Check the added amount on the confirmation screen. If it is correct, press 実行 (OK) and the charging procedures are complete.

4 Just hold up the mark on the mobile phone to the middle of the reader/writer, until you hear the "Clink" sound.

* The sound is for illustrative purposes.

* Initial settings are required to use "Edy" e-money.
* Prior service registration is required to charge Edy value via i-mode.
* Services other than "Edy" are available by downloading each i-appli beforehand.

E-money value can also be added at convenience store checkout points and other places where you can pay with "Edy".

Service is available at stores with the Edy mark

* The "Osaifu-Keitai" will clink when you shop.

In addition to Edy, another Osaifu-Keitai offering was "iD credit payment," "a credit card service that enables you to shop or withdraw cash by simply holding up your Osaifu-Keitai." DoCoMo Osaifu-Keitai Page at "iD credit payment service". As the following images from that 2006 English-language documentation show, the sign-up process required users to have a

compatible smartphone and an account with an affiliated credit card issuer. To enable the service on a phone, a user needed the authentication information acquired from the issuer. Once enabled, the phone and service could be used to make purchases.

iD credit payment service

iD credit payment service* is a credit card service that enables you to shop or withdraw cash by simply holding up your "Osaifu-Keitai". Just add this credit card function to your "Osaifu-Keitai" to enjoy a new level of convenience.
*This service is in Japanese only.

Main points of the Service

POINT 1 **You can shop with ease without the need to carry your card or need to sign*.**
*If the payment amount exceeds a set amount, you will need to enter your PIN.

POINT 2 **No need to prepay in advance.**
Because the "deferred payment method" means you pay the amount you have spent to the card issuer at a later date, you don't have the trouble of having to prepay in advance.

POINT 3 **Of course security features are included.**
For means of safety, you can set a password in case you lose your phone. (When the password feature is set, you will need to activate the "iD appli" and enter the password before you make a payment with iD credit payment service.)

Items Necessary for Use

In order to start the service, you will need to have an "Osaifu-Keitai", and you must apply at an iD compatible card issuer beforehand. (Before making initial settings on the mobile phone, you will need the authentication information you acquired when you applied to the card issuer in order to use the "iD".)

Sumitomo Mitsui card iD site (in Japanese only)

DoCoMo Mobile Credit Service "DCMX" (in Japanese only)

How to Use

iD credit payment service is available at stores with this iD mark.

Affiliated stores that accept iD (in Japanese only)

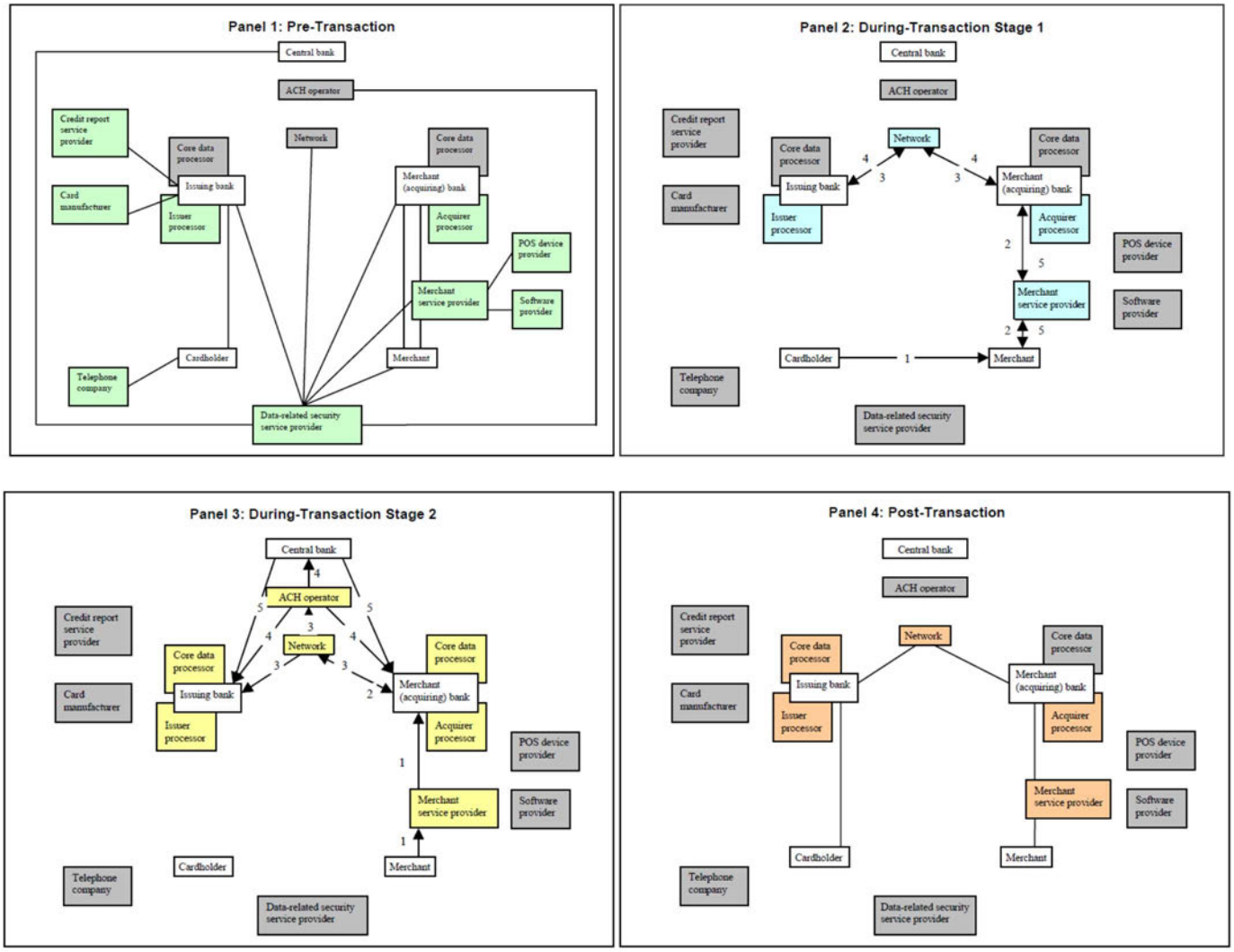
Wave the mark of your "Osaifu-Keitai" at a reader/writer at the store.

* If the payment amount exceeds a set amount, you will need to enter your PIN.
* If the reader/writer has difficulty recognizing the mark on your phone, try waving your handset in different directions.
* Packet communications charges will not apply when making a payment.
* If you are using the security feature, activate the iD i-appli and enter the password in order to unlock your phone before use.
* is a trademark of FeliCa Network, Inc.

4. Contactless Card Payment Systems Were a Foundation for Mobile Phone Payments

In a paper prepared for a May 2007 conference, the Federal Reserve Bank of Kansas City, presented "the initial results of a joint study undertaken by staff at the European Central Bank (ECB) and the Federal Reserve Bank of Kansas City to document and analyze nonbanks in the payments system," with a focus on "electronic (non-paper) retail payment services in the European Union (EU) and the United States." "Nonbanks in the payments system: European and U.S. perspectives," Payments System Research Working Paper PSR WP 07-01, Federal Reserve Bank of Kansas City, 2007, Abstract. The paper's figure 2, shows "the payment activities associated with a credit-card transaction over the MasterCard or Visa network that is initiated by a mobile

telephone. The figure has four panels corresponding to the four principal categories of payments activities: pre-transaction, during-transaction Stage 1, during-transaction Stage 2, and post-transaction." Id., p. 9.



5. Mobile Phone Payment Trials in Europe and the U.S.

Japan had an early start on NFC-based mobile phone payment systems, but in the 2000s there were numerous public tests and trials of such systems in the rest of the world. In May 2007, SecureIDNews listed fourteen that had taken place in Europe and the United States, with another four in China, Korea, Malaysia, and Taiwan. https://www.secureidnews.com/news-item/a-

sampling-of-nfc-pilots-from-around-the-world-2/. Four are listed below, and others are referred to elsewhere in these Invalidity Contentions.

In October 2006, credit card company JCB announced the successful launch of a trial in Amsterdam. It involved 100 customers with NFC-enabled Nokia phones and merchants provided with RFID-enabled payment terminals, where "cardholders can securely purchase items by just holding their mobile phone close to ViVOtech's contactless NFC reader/writer." https://www.global.jcb/en/press/2006/200610120001_products.html.

In February 2007, Discover and Motorola announced a test in which up to 1000 users in Chicago and Salt Lake City would be given NFC-enabled Motorola SLVR L7 phones to which they could download their Discover credit card accounts. Approximately 50 of the users were enabled to make contactless payments at retailers with NFC-enabled terminals. *See* https://investorrelations.discover.com/newsroom/press-releases/press-release-details/2007/Discover-Network-And-Motorola-Announce-Mobile-Payments-And-Account-Management-Trial/default.aspx, https://www.rfidjournal.com/news/discover-teaming-with-motorola-on-nfc-mobile-banking-trial/80033/, and https://nfctimes.com/project/us-early-trial-pairs-discover-motorola.

In October 2007, Kyocera Wireless announced the completion of a three-month trial in Jackson, Mississippi and Memphis, Tennessee, in which Cellular South customers were provided with NFC-enabled Kyocera phones equipped with fingerprint sensors / biometric authentication, and ViVOtech electronic wallet software. Customers downloaded credit cards into their phones via an over-the-air ("OTA") process, after which they could wirelessly pay for items at point-of-sale terminals at retailers utilizing NFC. https://americas.kyocera.com/press-releases/press-releases_201503201874.htm. Kyocera similarly exhibited and publicly displayed the technology

at the CTIA Wireless 2008 trade show in Las Vegas, NV. https://americas.kyocera.com/press-releases/press-releases_201503201967.htm.

In September 2008, UK mobile carrier O2 completed a 6-month NFC trial in which 500 Londoners were given Nokia 6131 NFC handsets with O2 Wallet software. Just under half of the users were also enabled to make contactless payments using their phones at retailers including Coffee Republic and Krispy Kreme. https://www.finextra.com/newsarticle/18919/london-nfc-trial-shows-customers-want-contactless-m-payments and https://newlaunches.com/archives/o2_nfc_put_to_trial_in_the_uk.php.

Samsung was also involved in NFC payment trials. A trial in Hagenberg, Austria ran from November 2006 through July 2007 and included 100 people being given NFC-enabled Samsung x700n phones. http://www.nfc-research.at/index.php@id=5.html. The phones could be used at six different payment points, including two cafeterias and four vending machines. *Id*.

Another Samsung phone, the SGH-D500E, was used in a 2005 NFC trial in Caen, France. *See* https://www.nfcw.com/nfc-devices/samsung-sgh-d500e-nfc/. Between 150 and 200 users could use the phones to make purchases at stores. https://nfctimes.com/project/france-orange-holds-early-multiapplication-trial, https://www.secureidnews.com/news-item/caen-france-hosts-worlds-premier-nfc-trial-with-mobile-phones-enabling-host-of-contactless-applications/ ("… residents in Caen will use [Samsung] mobile phones with an embedded Philips NFC chip as a means of secure payment in selected retail stores, parking facilities and tourist sites around town."). For retail applications, "Groupe LaSer Chains, which include Monoprix (supermarket) and Galeries Lafayette (department store), are equipped with NFC payment terminals enabling users to pay at checkout using their NFC phone. Along with more stores, the trial will eventually add a cashless payment scheme in partnership with Cofinoga, the consumer credit arm of Groupe LaSer,

said Mr. Duverne. Point-of-sale hardware from Ingenico powers the trial's retail payment environments." https://www.secureidnews.com/news-item/caen-france-hosts-worlds-premier-nfc-trial-with-mobile-phones-enabling-host-of-contactless-applications/.

G. The Use of Biometric-Enabled Phones Was Well-Known

The use of biometrics such as fingerprints has a long history. "In Asia, Europe and North America there are cave paintings which feature fingerprints possibly showing authorship and/or identity. In China there has been evidence of fingerprint impressions in clay which were then used for official documents. … In the Holy Roman Empire during the medieval period, wax seals bore deep fingerprints, usually three in a line." https://imprintproject.blogs.lincoln.ac.uk/2017/02/22/fingerprinting-as-an-identity-science-a-history/. Mark Twain included a chapter titled "A Thumb-Print and What Came of It" in his 1883 memoir "Life on the Mississippi," where he addressed the unique nature of thumb prints and how they can be used for identification. https://www.telelib.com/authors/T/TwainMark/prose/lifeonmississippi/lifeonmississippi31.html.

In the 1960s and 1970s, the FBI contracted with the National Institute of Standards and Technology (NIST) to study the process of automating fingerprint identification and subsequently funded the development of fingerprint scanners for automated classifiers, resulting in the development of the M40 algorithm and Automated Fingerprint Identification Systems (AFIS). https://ucr.fbi.gov/fingerprints_biometrics/biometric-center-of-excellence/files/fingerprint-recognition.pdf. By 1996, fingerprint scanners and biometric verification were so ubiquitous to the public consciousness that they were referenced in Mission Impossible:

Mission Impossible, 1996, character Sarah Davies bypassing a fingerprint scanner.

Mission Impossible, 1996, character Ethan Hunt using a retina scanner.

By 2001, fingerprint scanners were being included in commercially available laptops, such as the Acer TravelMate 739TLV and Compaq Armada E500. https://www.cnn.com/2001/TECH/computing/02/02/biometric.security.idg/index.html.

Fingerprint scanners were integrated into mobile phones at least as early as 2000, with the SAGEM MC 959 in 2000 (https://www.telecompaper.com/news/sagem-launches-mc-959-id-dual-band-gsm-handset--207905).

The 2003 Fujitsu F505i https://blog.greggman.com/blog/cell_phone_thumbprint_sensor/) and the 2004 Pantech GI100 (https://www.engadget.com/2004-08-03-stick-em-up-a-pantech-gi100-then-gimme-your-phone-and-your.html) also had fingerprint scanners.

In 2004 Fujitsu released the F900ic. Not only did this 3G phone include an integrated fingerprint scanner, it was also compatible with the above-described Osaifu Keitai system from NTT DoCoMo. *See* http://news.bbc.co.uk/2/hi/technology/3551070.stm; https://www.theflipside.info/f900ic.php.

The Kyocera Tempo E2000 was demonstrated at CTIA Wireless in 2008 and used in the above-mentioned NFC trial with Cellular South in a version that was NFC-enabled and included an integrated fingerprint reader. *See* https://americas.kyocera.com/press-releases/press-releases_201503201967.htm; https://americas.kyocera.com/press-releases/press-releases_201503201874.htm.

The Toshiba G500 and G900, both released in 2007, also had integrated fingerprint sensors. *See* https://www.mobilegazette.com/toshiba-portege-g500-g900-07x04x10.htm, https://www.cnet.com/tech/mobile/toshiba-portege-g900-and-g500-finger-friendly-smart-phones/, https://www.cnet.com/reviews/toshiba-portege-g900-review/. The G900 also included Bluetooth, Wi-Fi, and 3G connectivity, all discussed above.

The fingerprint reader on the back is surprisingly useful if you don't want to password protect the G900

The HP iPaq hx2790 did not have native cellular connectivity, but it did include Wi-Fi, Bluetooth, and a fingerprint sensor. *See* https://www.cnet.com/reviews/hp-ipaq-hx2000-review/.

A 2003 article discussed, at length, biometric and other security for handheld mobile devices. Jansen, W. (2003), *Authenticating Users on Handheld Devices*, Canadian Information Technology Security Symposium, May 12-15, https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=50736. It focused on:

> high-end Personal Digital Assistant (PDA) devices, having significant memory (at least 32MB flash and 64MB RAM) and processing speed (200Mhz or higher), aimed at corporate users. Usually, such devices come equipped with a one-quarter VGA touch screen and a microphone/ soundcard/ speaker, but lack a keyboard. One or more wireless interfaces, such as infrared or radio (e.g., Bluetooth and WiFi) are also built-in for communication over limited distances to other devices and network access points; so too are wired interfaces (e.g., serial and USB) for synchronizing data with a more capable desktop computer. Many high-end PDA devices also support Secure

> Digital (SD) and Compact Flash (CF) card slots for feature expansion. Over their course of use, such handheld devices can accumulate significant amounts of sensitive corporate information (e.g., medical or law enforcement data) and be configured to access corporate networks and resources via wireless and wired communications.

It reviewed "mechanisms, which are compatible with the capabilities of handheld devices and designed to facilitate user authentication, as alternatives to using passwords." *Id*. at 2.

> Password authentication is the most common example of a proof by knowledge procedure. Because of their simplicity and easy of implementation, password systems are the most ubiquitous form of user authentication. Though they are not completely free of problems, passwords nevertheless serve as the benchmark for assessing other authentication mechanisms.
>
> Smart card authentication is perhaps the best-known example of a proof by possession procedure. These credit-card-size, plastic cards host an embedded computer chip with its own operating system, programs, and data, and can be imprinted with a photo and other information, as well as a magnetic strip, for dual use as a physical identification badge [Pol97]. Many corporate security infrastructures incorporate smart cards.
>
> Fingerprint authentication is the oldest form of biometric verification and, thus, the best example of a proof by property procedure [Boe02]. A biometric is a unique, measurable characteristic of an individual, used to verify his identity. Biometrics, such as a fingerprint, by their very nature are impossible to forget and unlikely to be lost.

Id. at 2.

After recounting a bit of history and science about fingerprint identification (*id*. at 6-7), it discussed two commercially available options for use in handheld mobile wireless communication devices (*id*. at 7-8): the BioHub from Biocentric Solutions ("a small CF module that incorporates a fingerprint-imaging sensor … [with] software [that] controls biometric enrollment, matching, and access to a PDA. It also supports an option for file encryption.") and BioTouch from Identix, ("targeted mainly for notebook computers" with "a prototype solution for iPAQ PDAs"). "Fingerprint readers are also beginning to appear as built-in hardware on some PDA devices. For example, on HP's iPAQ H5450, the reader appears as a small strip beneath the navigation button." *Id*. at 8.

A September 2008 article in Scientific American noted that "[f]rom a commercial standpoint, one of the biggest advantages of using fingerprints is that the sensors for capturing prints are now extremely cheap (around $5) and small enough to be embedded in consumer products such as laptops, mobile phones and even flash-memory sticks" and that "laptops and mobile phones that can recognize a fingerprint, for instance, are now commercially available." "Beyond Fingerprinting: Is Biometrics the Best Bet for Fighting Identity Theft?", Jain and Pankanti, Scientific American, Sep 1, 2008, https://www.scientificamerican.com/article/beyond-fingerprinting/. It also noted that "[c]ompared with a physical token such as a bank card or with the knowledge of a secret such as a PIN, biometric traits are profoundly more difficult to forge, copy, share, misplace or guess" and that "[i]n some countries biometric security is employed to safeguard items such as ATM cards." *Id.*; *see also* https://biometrics.mainguet.org/types/fingerprint/fingerprint_history.htm.

H. Detecting and Enforcing Proximity Criteria

Conditioning functionality (including connectivity and messaging) to proximity is an age-old imperative. "Don't fire," said Colonel William Prescott, "until you see the whites of their eyes." This was in June of 1775, at the Battle of Bunker Hill in the American Revolutionary War.

WiFi, Bluetooth, IrDA, and some RFID implementations (including NFC) are considered short range protocols because a receiver and an emitter must be within tens of meters, or sometimes less than a meter, for communication to be successful. *See, e.g.*, https://www.jakelectronics.com/blog/an-overview-of-the-classification-of-wireless-network-technologies; https://www.mokosmart.com/short-range-wireless-communication-technology-vs-long-range-wireless-communication-technology/; https://ebyteiot.com/blogs/ebyte-iot-blog/7-short-range-wireless-communication-technologies.

Implementations of these protocols are inherent proximity detectors because of the short range of the signal: receiving a signal – or a signal of sufficient strength – indicates a degree of proximity. *See, e.g.*, this table from https://www.oracle.com/technical-resources/articles/javame/nfc.html, including the ranges of various communication mechanisms.

	NFC	RFID	IrDa	Bluetooth
Set –up time	<0.1ms	<0.1ms	~O.5s	~6 sec
Range	Up to 10cm	Up to 3m	Up to 5m	Up to 30m
Usability	Human centric Easy, intuitive, fast	Item centric Easy	Data centric Easy	Data centric Medium
Selectivity	High, given, security	Partly given	Line of sight	Who are you?
Use cases	Pay, get access, share, initiate service, easy set up	Item tracking	Control & exchange data	Network for data exchange, headset
Consumer experience	Touch, wave, simply connect	Get information	Easy	Configuration needed

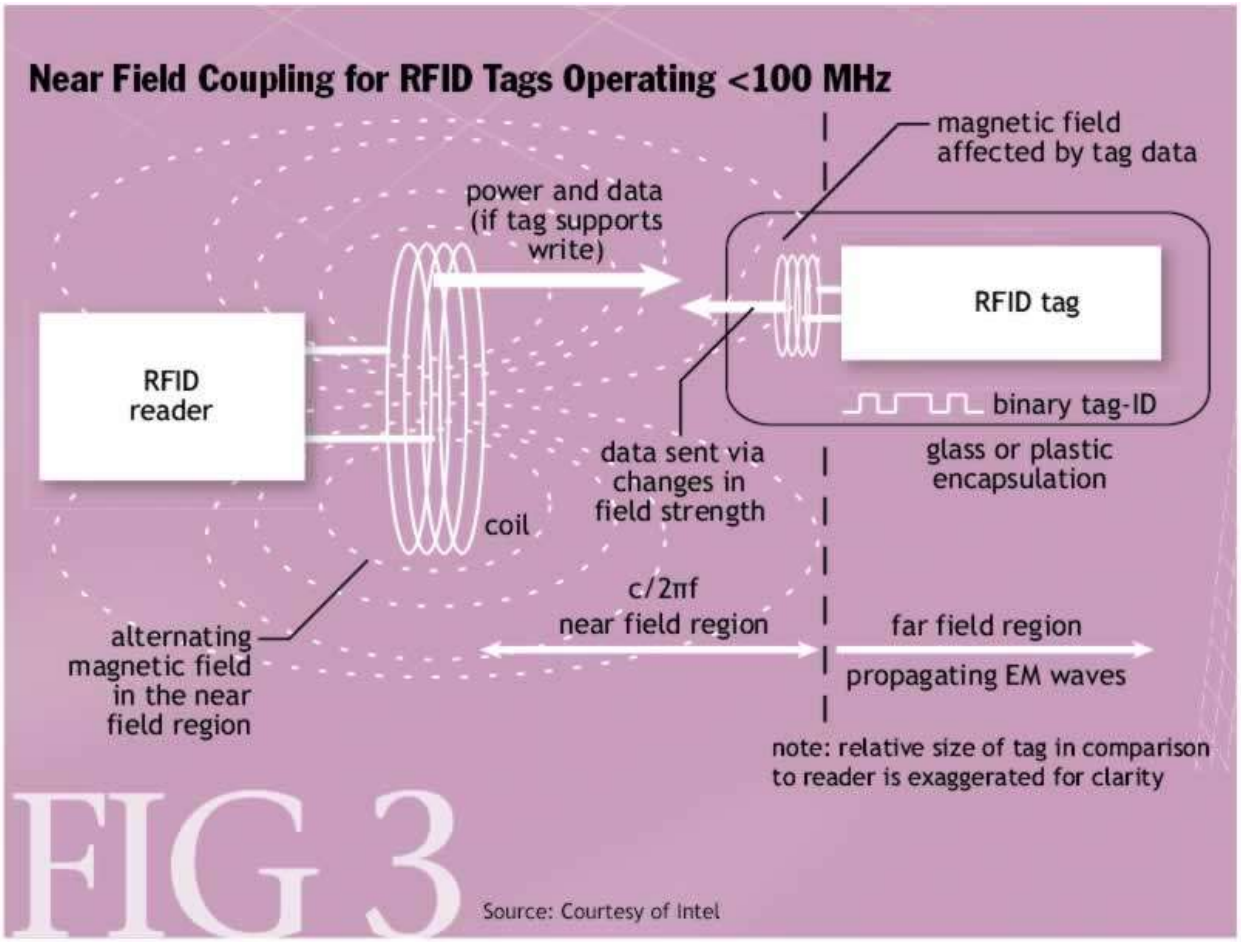
As explained above, Walton's 1973 patent leveraged this feature of RFID, and use of RFID in access keycards swelled in the years that followed. Similarly, the inherent proximity detection capabilities of RFID and NFC were leveraged in the toll and contactless smartcard systems discussed above.

A more technical description of why low frequency RFID tags (those operating up to 100Hz) are inherent proximity detectors available at, e.g., https://dl.acm.org/doi/fullHtml/10.1145/1035594.1035619. Roy Want. 2004. The Magic of RFID: Just how do those little things work anyway? Queue 2, 7 (October 2004), 40–48. Want explains:

> Passive tags that operate at frequencies up to 100 MHz are usually powered by magnetic induction, the same principle that drives the operation of household transformers. An alternating current in the reader coil induces a current in the tag's antenna coil, allowing charge to be stored in a capacitor, which then can be used to power the tag electronics. Information in the tag is sent back to the reader by loading the tag's coil in a changing pattern over time, which affects the current being drawn

by the reader coil—a process called load modulation. To recover the identity of the tag, the reader simply decodes the change in current as a varying potential developed across a series resistance.

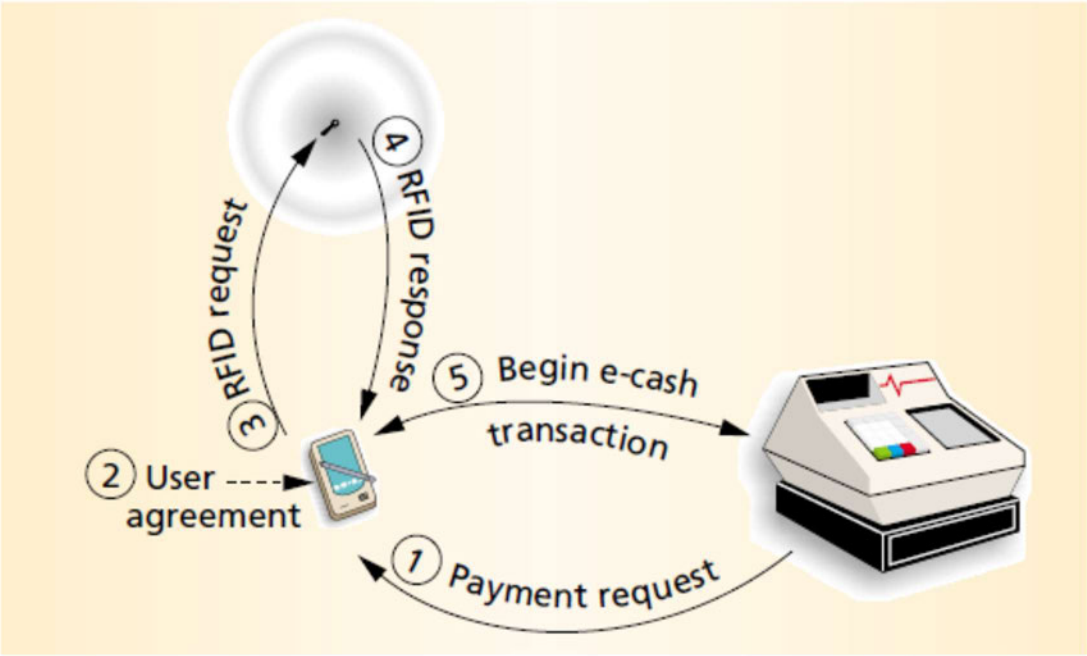
Unlike a transformer, the coils of a reader and a tag are separated in space, and coupling between the coils can occur only where the magnetic field lines of the reader coil intersect with the tag coil, the near field region (see figure 3). Beyond this distance the energy breaks away from the antenna as propagating waves that we call a radio signal; this is known as the far field region. The boundary of the near field and far field is governed by the frequency of the alternating current and is approximately limited to a distance of c/2pf; for example, at 13.56 MHz used by the ISO 15693 and 14443 standards, this distance is 3.6 meters, but at 915 MHz, used by EPCglobal, the range of the reader if based on near field coupling would be limited to six centimeters, reducing its usefulness.



Want explains that "In practice, at 13.56 MHz, most systems operate with a range between 1 and 30 cm, considerably shorter than the near field limit."

See also "RFID Systems and Security and Privacy Implications" by Sarma, Weis, and Engels. CHES 2002, LNCS 2523, pp. 454–469, 2003.

The use of a short-range signal detection as a means of establishing proximity detection was well known and assumed at the time of the alleged invention. For example, in "Parasitic Authentication To Protect Your E-Wallet," Thorne and Zheng discussed a transaction authentication system in which a user would have a second device in addition to their phone. Only if that second device was proximate to the phone, where proximity was determined by being in RFID communication, would the transaction be allowed. P. Thorne, T. Ebringer and Y. Zheng, "Parasitic Authentication To Protect Your E-Wallet" in Computer, vol. 33, no. 10, pp. 54-60, October 2000, doi: 10.1109/2.876293.

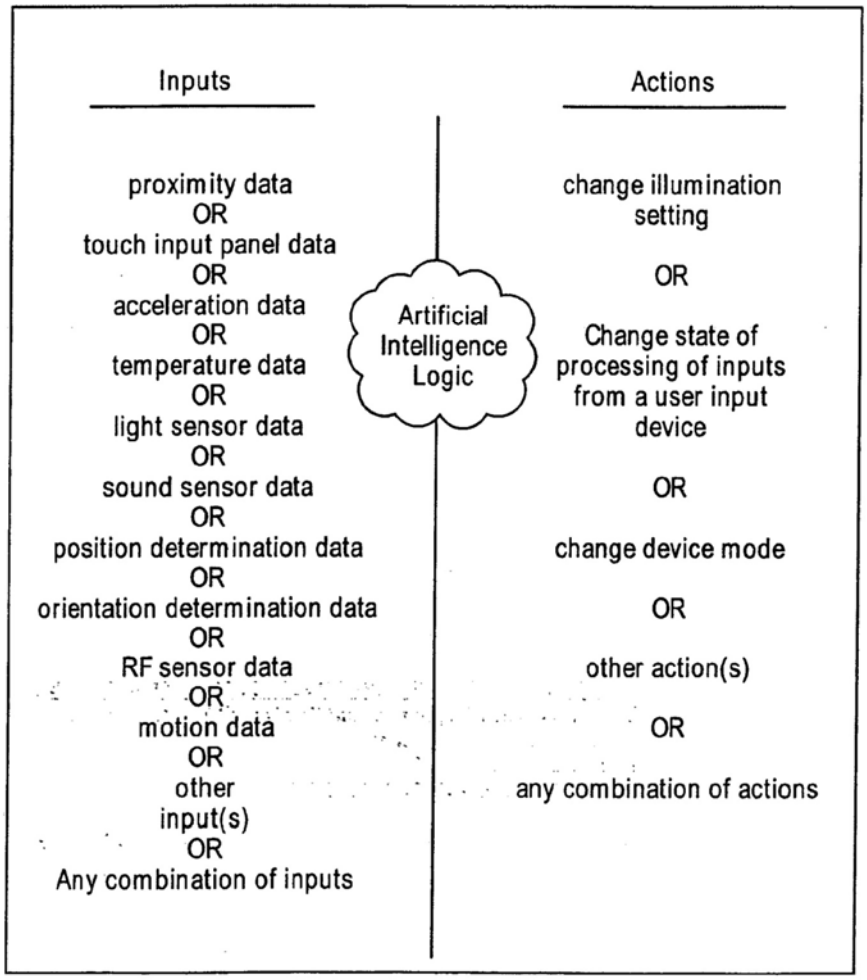


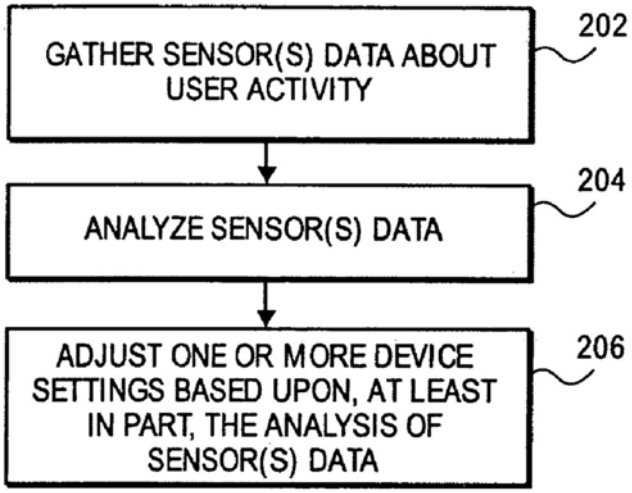
I. Blocking Mobile Phone Features or Functionality If Criteria Is Not Met

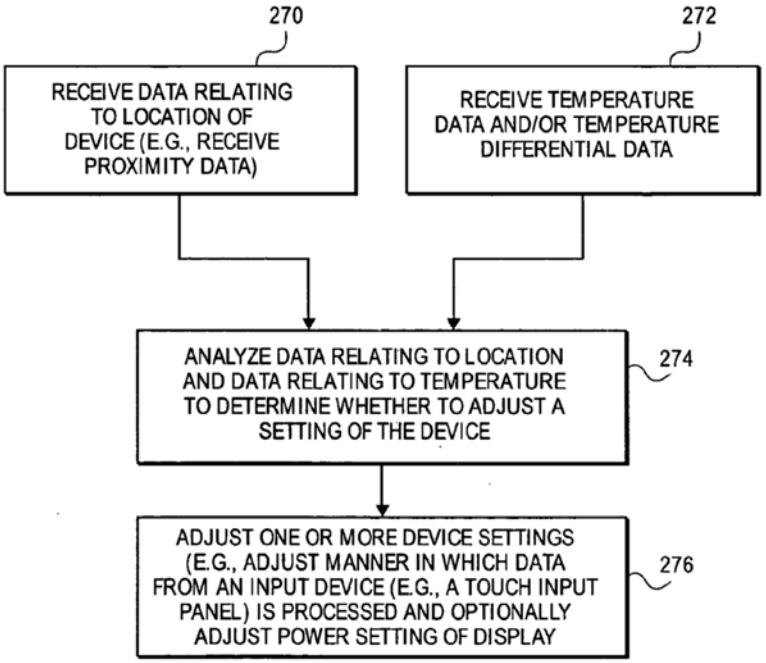
Dynamically enabling and disabling functionality, including communications, was well known at the time, even as applied to mobile phones.

A patent issued in 2005 based on an application filed in 2001 by engineers at Hewlett-Packard disclosed, among other things, a wearable device used to authenticate users for, *inter alia*, transactions. US6937135B2 (Kitson). The device had sensors that could be used to detect if it was being worn, and "[i]f the device 100 is not being worn, the device 100 may disable its authentication functionality and, thus, may prevent any secure transactions from occurring." *Id*. at 10:43-47. The device could also include wireless communications capabilities which could be used to connect to a verification service. *Id*. at 10:60-11:28. If data sensed by the device and provided to the service resulted in a determination "that the user's identity cannot be confirmed or that the user has not been in continuous possession of the device 100, such as where newly captured images do not match the baseline image … the device 100 may disable certain of its functions. Particularly, the device 100 may disallow certain transactions that require the authentication of the user's identity." *Id*. at 11:29-41.

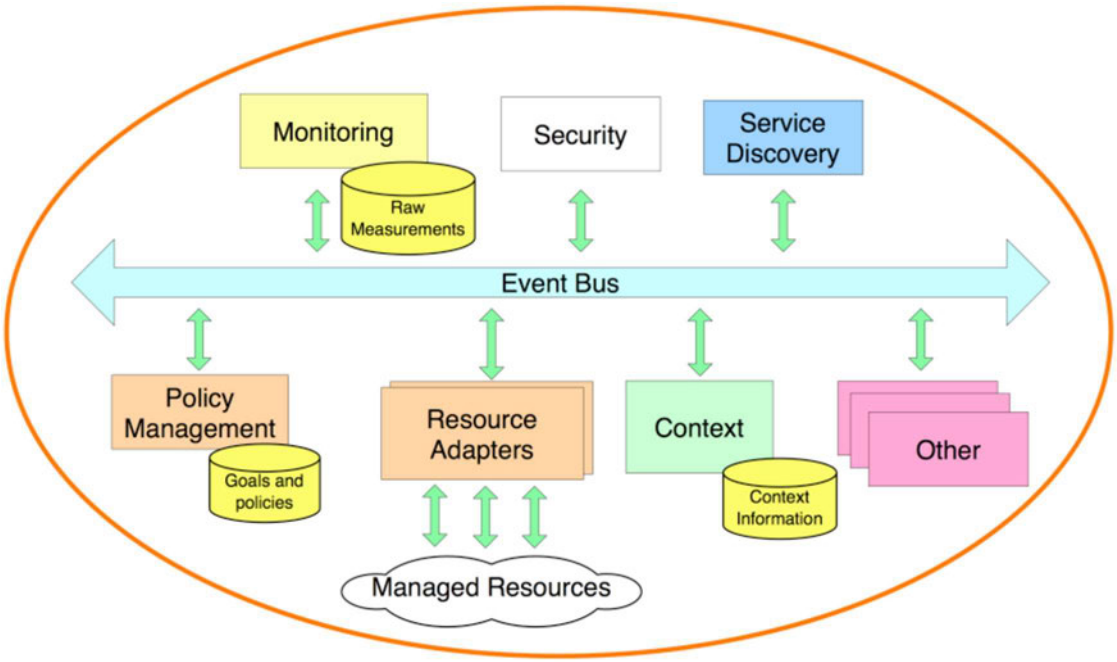
A 2006 patent application addressed improvements in long-established capabilities in this field. U.S. Patent Pub. 2007/0075965 ("Huppi"). Figures 8, 10, and 11D of Huppi show the basic concept: any number of inputs or combination of inputs can be processed to take any combination of actions.


Inputs
Actions
proximity data
OR
touch input panel data
OR
acceleration data
OR
temperature data
OR
light sensor data
OR
sound sensor data
OR
position determination data
OR
orientation determination data
OR
RF sensor data
OR
motion data
OR
other
input(s)
OR
Any combination of inputs
Artificial Intelligence Logic
change illumination setting
OR
Change state of processing of inputs from a user input device
OR
change device mode
OR
other action(s)
OR
any combination of actions


GATHER SENSOR(S) DATA ABOUT USER ACTIVITY
202
ANALYZE SENSOR(S) DATA
204
ADJUST ONE OR MORE DEVICE SETTINGS BASED UPON, AT LEAST IN PART, THE ANALYSIS OF SENSOR(S) DATA
206



A January 2007 paper, Policy-based Management for Body-Sensor Networks ("Keoh"), described the design and implementation of a system in which on-body wireless sensors communicated with mobile phones and other wireless devices, which could then process the input and send updated rules and policies to the sensors.



The paper concluded: "The ability to dynamically load, enable and disable the policies together with the ability to use policies in order to manage other policies caters for a wide variety of application needs. … The ability to provide a constrained form of programming such as policies is equally important at the individual sensor level. It enables adaptive behaviour of the sensor according to context and thus to also adapt computational requirements and communication and hence power consumption… the resulting principles and framework developed are equally applicable to other application areas such as unmanned vehicles, ad-hoc networks, virtual collaborations as well as network and systems management." *Id*.

In June of 2008, Research In Motion, makers of the Blackberry, applied for a patent reciting "a mobile device may be provided that is configured to have at least one function disabled when the speed of the mobile device exceeds a threshold. The mobile device includes an output component configured to provide a notification related to disabling the at least one function. The mobile device may also comprise a first input component configured to promote controlling whether to disable the at least one function." EP2099203 ("Dietz") at [0002]. In particular, it disclosed that "[w]hen the speed of a mobile device is determined to be above a threshold, an assumption can be made that the device is in a moving vehicle. The mobile device's transmitting and/or receiving capabilities might then be disabled, the device's user interface might be disabled, or other restrictions might be placed on one or more of the device's functions." *Id*. at [0013].

Also, many of the phones and wireless devices with integrated fingerprint sensors, including but not limited to those discussed above, had lock modes that could be disabled using biometrics. *See, e.g.*, https://web.archive.org/web/20040603211821fw_/http://www.sagem.com/en/communiques-

en/cp-2000-en.htm (including January 24, 2000, press release: "Fingerprint recognition replaces the PIN code to customize the GSM mobile and prevent fraudulent use if lost or stolen").

J. Wallets, Over the Air (OTA) Authorization, and Future Financial Transactions

Some of the discussions above already demonstrated the prior use of digital wallets to store payment credentials on a mobile device and over-the-air authorization or personalization of mobile devices to use payment mechanisms. This section elaborates on that. Additional examples of wallets and OTA processes are set forth in the invalidity charts that are part of these Invalidity Contentions.

In 2000, Thorne et al. published "Parasitic Authentication To Protect Your E-Wallet" in IEEE's Computer magazine. It began by noting "[t]he electronic wallet (e-wallet) has received much attention lately. It promises to consolidate many of the personal items carried around by the modern individual: wallet, phone, pager, diary, and keys. In fact, Nokia's 9001 Communicator already combines the phone, pager, and diary into one unit." (Page 2.) The paper focused on security issues related to e-wallets, which it defined as a system able to "hold[] identification information such as a driver's license, facilitate[] two distinct payment systems (cash and credit), and act[] as a repository for temporary tokens such as bus tickets." *Id*. For example, it explained a biometric approach, whereby the e-wallet "would not perform a transaction unless a valid fingerprint is scanned." *Id*. at 3.

A 2004 patent application by Staib et al. (published as US 20050222961A1) discussed "electronic payment systems for portable devices that act as smart cards." [0002]. It reviewed prior use of such systems in the United States and elsewhere, including ISO 14443 and other suitable technologies and the above-mentioned FeliCa and Speedpass systems. [0003]-[0013]. The application observed, at [0017], that at the time "the applications in the contactless payment device

are designed based on the specific requirements, such as data exchange, security, and settlement, of that specific contactless payment system, which are different for each contactless payment processing system." "Therefore," it continued, " it is desirable to provide a contactless payment system that links multiple payment systems to allow a user with a single mobile contactless device to pay for good and services that are provided across different contactless payment systems." [0019].

Staib summarized its own solution at [0021]-[0024]:

> According to the principles of the present invention, a system for facilitating contactless payment transactions across a plurality of different contactless payment systems using a common mobile device that acts as a stored value device is provided. A mobile application running in the mobile device is associated with one contactless payment system. While the mobile device is not associated with other contactless payment systems, it can nevertheless perform contactless payment transactions with merchants that are associated with those other payment systems by emulating the transmission standards and data exchange formats used by those payment systems. Once the transactions take place, a service application running in a service operator's computer communicates with the various contactless payment systems to settle the amounts owed to other contactless payment systems by the one contactless payment system that is associated with the mobile device. The combination of the mobile application and the service application provide a complete solution to allow a common mobile device to pay for goods and services through merchants that are associated with different payment systems as well as subsequent settlement of payments among the different payment systems.

Starting at [0044] it introduced the OTA authorization or personalization process, which in one embodiment involved downloading a secure application that facilitated that process:

> A contactless payment transaction involves the following players: service operator 48, wallet operator 50, users who subscribe to the payment services of the service operator, financial institutions 49 holding deposit accounts of the users, and merchants 22 who provide goods or services.
>
> The service operator 48 provides the software and information technology requirements of the payment clearing service of all purchase transactions. The wallet operator 50: 1) receives customer's money on its bank account from the customer's bank during the initial load and top up of the stored value; 2) pays the merchants 22 or the contactless payment networks with roaming agreements for customer's transactions; 3) converts stored value into foreign currency when the customer goes abroad and coverts it back into home currency when the customer returns; 4) pays

> wallet operators of different contactless payment systems whether they are located in other areas or the same areas. The functions provided by the service operator 48 and wallet operator will be explained in detail later herein.
>
> Initially, a user signs up for a contactless payment service with the service operator 48. The wallet operator 50 has an existing arrangement with the bank 49 holding the user's deposit or credit card account (see FIG. 8). During sign-up, a predetermined amount of money is transferred into a bank account of the wallet operator 50 and is written into the secured area of the memory 15 of the smart mobile device 10 as a stored value. The mobile device 10 is now associated with a particular payment system or network such as shown in FIG. 3 which shows the merchant 22, mobile device 10, service operator 48 and wallet operator 50 all associated with a single payment system or network. The merchants 22 have an existing arrangement with the service operator 48. Once goods or services have been rendered, the merchant 22 presents a payment request to the wallet operator 50.
>
> The wallet operator 50, which essentially acts as a bank, may be a part of the service operator 48 or a separate entity that has an existing agreement to handle all financial aspects of the contactless payment transactions for the service operator 48.

At payment time, one option was for the phone to automatically determine what payment to use, although various other approaches are disclosed in subsequent paragraphs.

> [0052]: In step 34, the user is ready to purchase an item. The user places the mobile device 10 near the contactless communicator 12 to initiate a payment for the purchase of the item. At the merchant location 22, a merchant application 39 is stored in the memory of a merchant computer 100. In step 36, the contactless communicator 12 queries the mobile NFC device 10 for the stored value stored in the mobile device. At that point, the mobile device 10 together with the mobile application 2 determines the payment system in use by the merchant and places the mobile device in an emulation mode to emulate the transmission standard and data exchange format used by the merchant 22.

By 2005, Chameleon Networks had released Pocket Vault. This was a biometrically protected device that could imprint a reusable Chameleon Card with information corresponding to numerous credit, payment, or other cards whose information a user had downloaded or entered into the Pocket Vault. *See, e.g.*, https://web.archive.org/web/20040602202951/http:/chameleonnetwork.com/pocket_vault_info.htm; https://gizmodo.com/chameleon-card-and-pocket-vault-8677 (March 5, 2004); https://coolhunting.com/tech/pocket-vault/; https://www.wired.com/2004/03/chameleon-card-

changes-stripes/; "Out-of-Pocket Relief" in the May 2004 issue of Strategic Finance, and https://web.archive.org/web/20040603023030/http:/www.wired.com/news/business/0,1367,62545,00.html?tw=wn_tophead_7.

In February 2006, Motorola announced M-Wallet. *See* https://www.cnet.com/tech/mobile/motorola-to-launch-new-mobile-wallet-service/. A CNET article documenting the announcement reminded readers that "[t]he roots of the new M-Wallet service, which is coming to North America, are in Japan, where companies like Japanese wireless carrier NTT DoCoMo began issuing mobile wallets two years ago."

Innovision's 2006 whitepaper "Near Field Communication in the real world: Turning the NFC promise into profitable, everyday applications" observed that "[b]anks and mobile network operators are very interested in putting payment and ticketing applications on NFC-enabled mobile phones." (Page 8). It cited research conducted by Visa as finding "89 per cent of those who tried phone-based transactions preferred its convenience to alternative payment methods." *Id*. It asserted that mobile wallets on NFC-enabled devices "would replace the myriad credit, debit, loyalty, pre-paid and other cards that people carry around in their wallets today." *Id*.

ViVOtech's RF-Based Contactless Payment whitepaper, already version 3.0 by 2006, stated that "all major card associations have started their own contactless payment programs" in the United States, noting that American Express piloted ExpressPay in 2003 (and launched a contactless card in the United States in 2005), that MasterCard trialed PayPass the same year, that in Q4 2005 Visa announced its strategy, and that Discover was expected to do so later in 2006. ("RF-Based Contactless Payment" ViVOtech White Paper version 3.0, April 2006 at page 6). The whitepaper described ViVOtech's ViVOnfc Software Suite, which included ViVOplatform provisioning server: "An over-the-air (OTA) provisioning infrastructure which allows issuers to

securely download a variety of 'soft cards' over the carrier's radio spectrum into NFC phones. These include credit, debit, prepaid, loyalty, and gift cards as well as mCoupons, event tickets, parking and transit passes." It also included ViVOwallet, which "allows consumers secure access to their soft cards directly from their mobile phone display" and "provides transaction reporting functions such as balances, payments history, and content discovery from smart posters." (Page 28).

ViVOnfc Software Suite Components

ViVOplatform Provisioning Server: An over-the-air (OTA) provisioning infrastructure which allows issuers to securely download a variety of "soft cards" over the carrier's radio spectrum into NFC phones. These include credit, debit, prepaid, loyalty, and gift cards as well as mCoupons, event tickets, parking and transit passes.

ViVOplatform Issuer Server: A secure server installed at card issuing financial institutions that enables secure download of credit card information directly from the issuing bank directly into a encrypted smart chip embedded in the NFC-enabled phone.

ViVOwallet Software: allows consumers secure access to their soft cards directly from their mobile phone display. This software also provides transaction reporting functions such as balances, payments history, and content discovery from smart posters.

Midlet Payment Software Package: that provides secure communications between the NFC phone and the growing number of merchant locations that are being equipped to accept Contactless payments.

In November 2006, MasterCard, Nokia, and 7-Eleven conducted a trial in Dallas in which participants received a Nokia 3220 phone "with instructions on how to provision it with MasterCard's PayPass service. Users have their banks provide information to setup eFinity prepaid accounts that are accessed at 7-Eleven stores, McDonald's, some professional sports stadiums and other retail outlets that accept PayPass for purchases under $25. Once the prepaid account is established, G&D's platform sends data over-the-air to provision the phone. The phone can be password protected to prevent financial loss if lost or stolen." https://www.rcrwireless.com/20061103/archived-articles/mastercard-nokia-again-team-for-nfc-payment-tests. One goal "is to test the effectiveness of Giesecke & Devrient's over-the-air NFC

account-payment configurations solution, designed to enable consumers to dial up a specified phone number and quickly link a payment account, such as a credit- or debit-card account, to an NFC-enabled phone. This allows them to use the phone just as they would use an RFID-enabled payment card. To get previous NFC technology trials up and running, project architects configured the payment accounts on behalf of the testers. While this approach made the pilots easy to deploy, it is not one that could scale to a mainstream deployment with thousands or millions of participants." https://www.rfidjournal.com/news/mastercard-and-7-eleven-launch-nfc-trial/80201/.

A February 14, 2007, article in RFiD Journal explained that Discover and Mastercard were conducting a trial in Chicago and Salt Lake City that included Motorola's M-Wallet software on Motorola mobile phones:

> Sokhey says the M-Wallet platform will make it easier for wireless carriers to begin offering and supporting NFC-enabled phones. Rather than having to support the Visa, MasterCard, Discover or other contactless payment technology platforms separately, the carriers can just offer Motorola phones with M-Wallet, which can support all of the unique payment specifications (including data security protocols) under one umbrella.
>
> "M-Wallet is credit-card-agnostic," Sokhey explains, "and can support up to 50 different [types of] cards." He says Motorola and Discover are working with Ztar, a Dallas-based mobile virtual network operator, to provide the cellular service for the phones used in the trial. To pull their Discover account information onto the NFC module inside the phone (where it is stored as encrypted data), trial participants employ an over-the-air NFC initialization function that is part of the M-Wallet platform.

https://www.rfidjournal.com/news/discover-teaming-with-motorola-on-nfc-mobile-banking-trial/80033/; *see also* https://www.securetechalliance.org/discover-network-and-motorola-announce-mobile-payments-and-account-management-trial/.

The Smart Card Alliance observed in 2007 that "Recent proximity mobile payments pilots download a payment application dynamically to the phone's SIM or secure element, using OTA,

as required by the consumer. Unlike a standard activation, this process is not under the control of the mobile operator, nor can it be managed by the typical personalization process implemented by financial institutions." ("Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure", p. 15). On pages 16-17, it described a "proximity mobile payment implementation scenario" in which "multiple payment cards could be supported by the mobile phones currently being developed and tested by handset manufacturers":

> Consumers can then carry their choice of payment cards on the NFC phone and choose a payment option at the time of purchase, just as they do today using a physical wallet or purse and plastic cards. The payment cards present on an NFC phone can be thought of as "soft cards." They reside on the phone in electronic form and are managed by a secure wallet software program. The wallet software may display images of the soft cards that incorporate the card issuer's branded look and feel, as on a plastic card. The program can display these images at the time of a purchase. Consumers choose a payment card by selecting an image.
>
> Financial information, such as an account number and expiration date, is stored in a secured memory area in the NFC phone. This memory could be provided either by a secure smart card chip similar to the one used for contactless payment cards (currently implemented in most of the NFC-enabled mobile phone pilots), in the memory of the SIM chip (which is used by GSM mobile phone operators to authenticate subscribers on their network and maintain personalized subscriber information and applications) or in another secure element in the mobile phone. Vendors are currently offering SIMs with additional cryptographic capability that allows for secure storage not only of financial data, but also of the branded contactless payment applications being supported by the financial industry.
>
> Consumers could request that soft cards be issued OTA by clicking a few buttons on their NFC phones and identifying themselves to the issuers as the correct cardholder. Enhanced OTA management capabilities could enable issuers to activate cards or cancel lost, stolen, or over-limit cards. To facilitate OTA issuance, mobile phone operators will need to work with major financial payment card issuers to develop a consumer activation process. The OTA infrastructure currently deployed by mobile operators can support OTA activation of soft cards. However, inter-network communication and security protocols must be standardized, and the card issuers and operators must develop a business model that benefits all participants in the payment transaction.
>
> Upcoming pilots are testing several different personalization and issuance models. Regardless of the model, it is expected that all stakeholders could see multiple benefits

> from the deployment of remote mobile payment using soft cards. These benefits are discussed further in the following sections.

Then, in a discussion of the business models mobile operators might see in a US mobile payment system, it noted "the incorporation of a single integrated mobile wallet that enables a consumer to add any payment card from any financial institution desired may provide the foundation for an additional revenue source. For example, with this model, the operator may be able to generate advertising revenue through the impressions presented to the consumer when using such a wallet." (page 23).

On page 24 it provided more context for OTA, including that multiple OTA solutions might invite demand for consolidated "trusted service managers:"

> Provisioning cards in a mobile phone environment presents new challenges. One major challenge is that there are hundreds of mobile phone form factors. Sending cards through a defined manufacturing process is not feasible. Another challenge is that in most cases, a card in a phone will not be personalized until after the phone is in the user's hands. Currently, cards are personalized when they are issued and the user simply calls a number to activate the card.
>
> These two issues have resulted in the development of OTA provisioning and personalization services. These services provision consumer applications to a consumer's NFC-enabled device. The applications can be credit, debit, or prepaid payment cards. They can also be transportation cards or event tickets.
>
> OTA provisioning services introduce the need for a trusted services manager (TSM). The main role of the TSM will be to aggregate the applications from different service providers and perform card management and OTA provisioning to the secure element of the handset. In some cases, the mobile operator will act as the TSM. In other cases, the TSM will be a trusted third party.
>
> ***
>
> The secure element can be a secure microcontroller embedded in the handset (either mounted on the motherboard directly or connected in some way to the motherboard). This is the architecture that has been most widely tested in mobile payments field trials around the world. The advantage of this approach is that the secure elements that can be embedded today have all the necessary banking hardware and software certifications. One concern facing this option is how to manage the replacement of the handset when the subscriber wants to change their phone. The transfer of payment credentials could be managed OTA in the same way that the secure element is

initialized. This provides another service revenue opportunity for the operator and/or the trusted service manager. (p. 24)

A few months later, in July 2008, the SCA published "Proximity Mobile Payments Business Scenarios: Research Report on Stakeholder Perspectives." This paper quotes an industry participant saying: "Consumers will want more choice – they will want a wallet that holds the same cards they have in the actual wallet. So consumers will drive toward more than one financial institution. Would be confusing to have multiple wallets on the same phone." (p. 15). That report defined "mobile wallet" as "A software application that is loaded onto a mobile phone for the purpose of managing payments made from the mobile phone. A mobile wallet application can also be used to hold and control a number of other applications (for example, payment and loyalty), in much the same way as a physical wallet holds a collection of physical cards" (p. 33).

Among the earlier implementations of OTA are:

- "In February 2007, MasterCard, in cooperation with Taiwan Mobile, Taipei Fubon Bank, and ViVOtech, launched MasterCard PayPass in mobile phones in Taiwan. MasterCard worked closely with the industry to leverage NFC and over-the-air (OTA) technology to allow Fubon Bank cardholders to download PayPass cards and promotion coupons to their NFC-enabled phones" ("Proximity Mobile Payments: Leveraging NFC and the Contactless Financial Payments Infrastructure," p. 8).

- "In February 2007, Visa and SK Telecom announced plans to launch what is expected to be the world's first mobile contactless payment using a Universal SIM card personalized OTA. This solution is based on Visa's mobile platform. This large-scale service will initially involve 30,000 SK Telecom subscribers and 50,000 point-of-sale locations." (Id., p. 9).

- "In January 2007, HSBC launched a mobile phone payment pilot in partnership with MasterCard and ViVOtech. Using a simple OTA personalization process, participants in New York, Chicago, and several other large U.S. cities loaded their HSBC credit cards onto their mobile phones. Participants are able to use their NFC phones at thousands of PayPass-enabled merchant locations nationwide. Recently, HSBC has extended the pilot to allow its debit cards to be downloaded onto NFC mobile phones, resulting in the first multi-card NFC mobile phone pilot." (Id. p. 10).

Two 2007 patent applications by Beenau et al., then with American Express, also discuss wallets and OTA authorization. US 8543496 (Beenau 496) and US 8620260 (Beenau 260) (each

incorporating the other by reference). Beenau 496 begins by acknowledging what already existed and identifying targets for improvement:

> A mobile phone user who has a transaction account such as an American Express®, Visa®, MasterCard®, or Discover® account can adapt the phone for use as a payment device in one of several ways currently in development.
>
> For example, the user can visit a secure website in order to request that a payment application and personal account information be transmitted to the user's mobile phone. In this method, the user might provide his or her transaction account number, the telephone number of the user's mobile phone, and verification information (such as personal information or a password) at a computer connected to the Internet. When the provider of the transaction account receives the user's information over the Internet, the provider verifies the information and preferably associates the user's transaction account number with the telephone phone of the user's mobile phone.
>
> …
>
> In each case, after the provider verifies the received information and preferably associates the user's transaction account number with the telephone number of the user's mobile phone, the user is able to download a payment application to the mobile phone and to use the mobile phone as a payment device.
>
> Typical downloading methods can be used, such as by plugging the mobile phone into a computer in which the necessary software has been stored, or which can provide a conduit to an Internet site at which the software is located.
>
> …
>
> There is, however, a need in the art for an improved method of operating a mobile phone application. There is also a need to provide security features to the payment application on a mobile phone that has been enabled for use as a payment device, in order to enhance user experience and confidence in the payment application.

Beenau 496 summarized its contribution as improving how "a mobile phone can function as a payment device as well as a device for making telephone calls and the like. Thus, the phone can conveniently be used as a financial transaction instrument in lieu of a traditional financial transaction instrument, such as a credit card."

It presented OTA authorization: "a method of operating a mobile phone having financial transaction account information of a user, an application for operating the mobile phone, and a

transmitter for transmitting information of the user to a reader… receiving financial transaction account information of the user and transaction information of a financial transaction, processing the received information, and communicating with the user's mobile phone over a wireless network to receive and/or transmit information related to the transaction information." 2:15-39. It elaborated on this in more detail at 7:4-9:8. In one embodiment, the process culminated when "the secure element in the phone has been personalized with the financial transaction account information." 8:40-45.

The entire process "can be repeated for a plurality of financial transaction accounts, such that the mobile phone can be used in placed of multiple financial transaction instruments. In this way, the mobile phone user can avoid the need to carry numerous traditional cards in order to purchase a variety of goods and services from different types of merchants." 9:9-15.

Beenau 260 reinforced some of these points, noting at 9:18-36:

> [T]here is no need to plug (or otherwise physically connect) a mobile phone into a computer in order to enable the phone to function as a mobile payment device. The downloading of the description file (108), the downloading of the resource file (109), and the downloading of the personalized data p`ackage (110) preferably all occur over a wireless network. Further, secure personalization is fast. For example, the process from the user's receipt of the SMS message (sent in step 107) to complete download of the personalized data package (sent in step 110) onto the user's mobile phone may take about a minute. Moreover, the URL in the SMS message is easy for a user to use, and the user is able to make as little as a single "click" (on the URL in the SMS message) in order to enable a mobile phone to function as a mobile payment device. As well, secure personalization of a payment application according to the present invention does not rely on an online connection to a host server, avoiding problems such as incomplete downloads due to dropped connections.

In a February 2008 patent application (published as US2009/0037326), Chitti et al. (of Motorola) discussed "virtual cards stored in a portable electronic device, and more specifically to a method and apparatus for arranging or selecting virtual cards stored within an electronic wallet." [0003]. They provided this background at [0005]-[0007]:

> Due to rapidly advancing technology, paying for goods and services is becoming faster and more effortless. Not long ago, when a person wanted to purchase goods or services, they had to physically hand cash or a hand-written check to a cashier. The advent of magnetic striped credit cards simplified this process, as a person was able to "swipe" a credit card having a magnetic strip through a payment terminal in lieu of giving cash or a check to a cashier.
>
> The advent of radio frequency "contactless" communication technology simplified the process even further. With contactless technology, rather than having to swipe a plastic card having an easily damaged magnetic strip through a narrow slot, a person is able to simply wave a card or key fob equipped with a hidden embedded computer chip and radio frequency antennae within an inch or two of a reader. Information, such as account number, expiration date, and account holder, is then transferred wirelessly to a reader to complete the financial transaction. When using such technology, to make the process even simpler, many merchants require no signature or personal identification number for small purchases, such as those less than twenty-five dollars.
>
> Even with contactless technology, making purchases can be still somewhat cumbersome. For instance, when a user has multiple contactless-enabled cards in a wallet, the specific card to be used must be removed from the wallet and passed over the reader. Similarly, for the person who prefers key fobs, when that person carries multiple key fobs, the specific one used to make a purchase must be separated from the collection and passed over the reader.

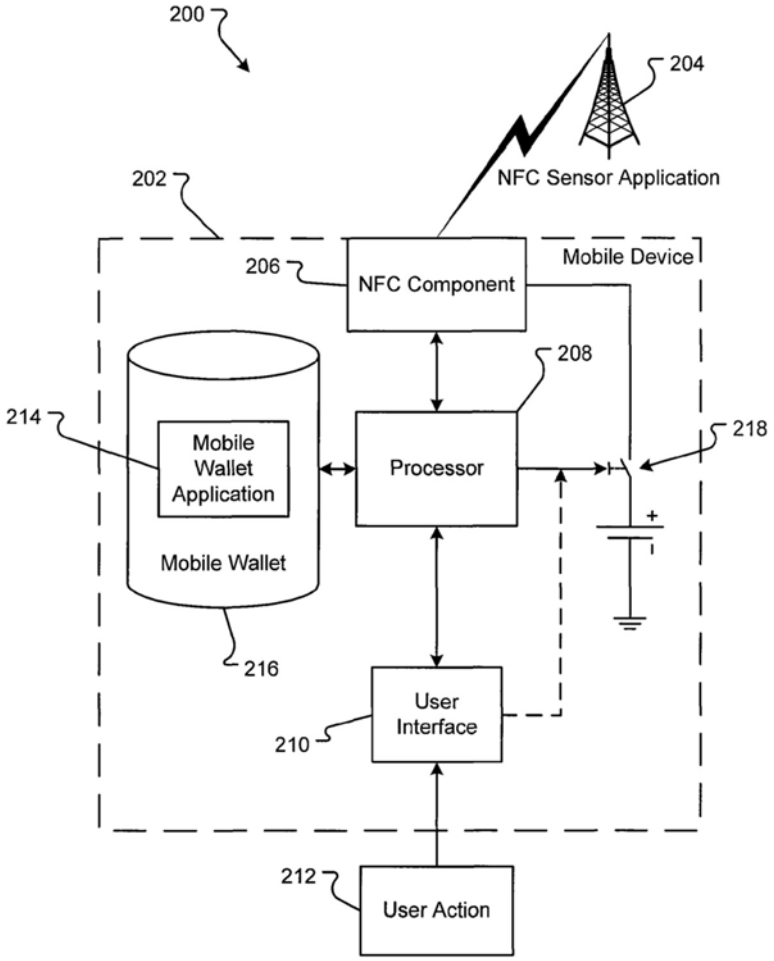
At [0023]-[0025] they reviewed that users could OTA authorize multiple payment mechanisms, cluttering digital wallets.

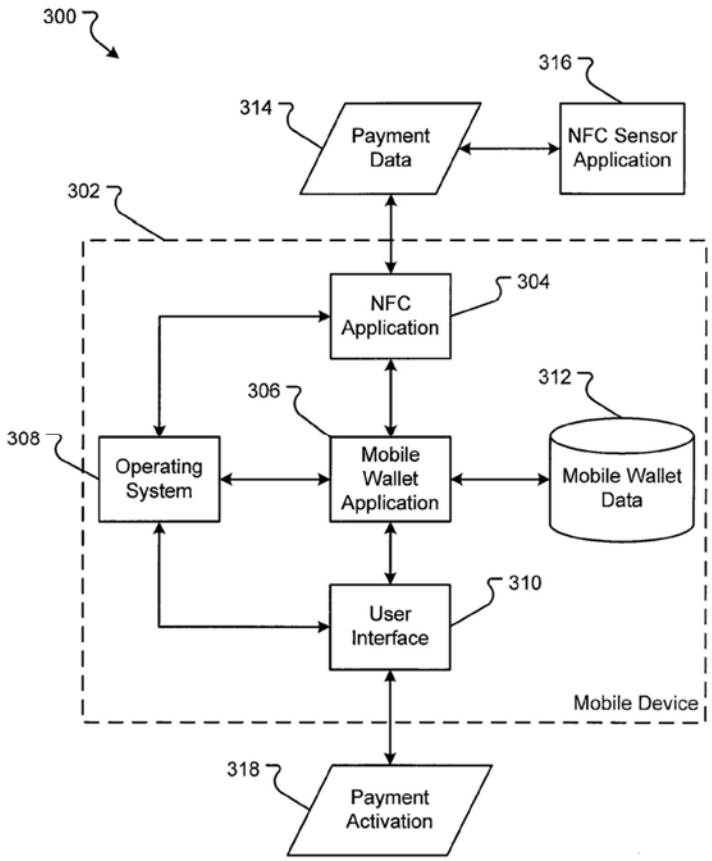
> Some mobile device manufacturers have recently developed electronic, or "virtual," cards. For example, Mastercard®, in conjunction with some mobile phone manufacturers, offers a virtual "PayPass" card that is stored within the memory of a mobile telephone. In some embodiments of a mobile device, this card is stored within a secure memory, secure region of memory, or within a memory associated with a secure processor. Storage in within a secure element in the mobile device helps guard against unauthorized use of the information. The virtual card is loaded, installed, and personalized with card specific information, such as account number, name, expiration date, and one or more secure keys. The mobile device then transmits the information wirelessly to payment terminals via a near-field transceiver. The payment terminal is thus able to access the information and bill the user for a purchase.
>
> As one virtual card can be stored within a device, so can others. To select the proper card to use, a user must navigate through a series of menus to find the virtual card application. Once in the application, the user must scroll through the various virtual cards and select the proper one. For some cards, additional information must be entered, including personal identification numbers and security codes. Such a process is cumbersome.

> Embodiments of the present invention streamline the process and offer the user a more seamless experience with virtual cards. In one embodiment, the invention includes a "virtual wallet", which includes a virtual card software application, running within the device, that hosts different cards (credit, loyalty, membership, identity, etc.). The virtual card application manages the virtual cards and permits user selection of the cards as well. The virtual wallet may further facilitate displaying the cards on a display in a wallet-type image.

In July 2008, Skowronek and others affiliated with First Data Corp filed the application that resulted in U.S. Pat. No. 8,662,401. After recognizing the widespread availability of contactless payments and the use of wallet applications, Skowronek purported to address perceived security issues by allowing users to exercise control over a wallet application so that it would not start or activate even in the presence of an NFC field. *See* 1:27-37 and 2:3-20.

Skowronek Figures 2 and 3 showed mobile wallet applications in the context of a payment device like a smartphone:

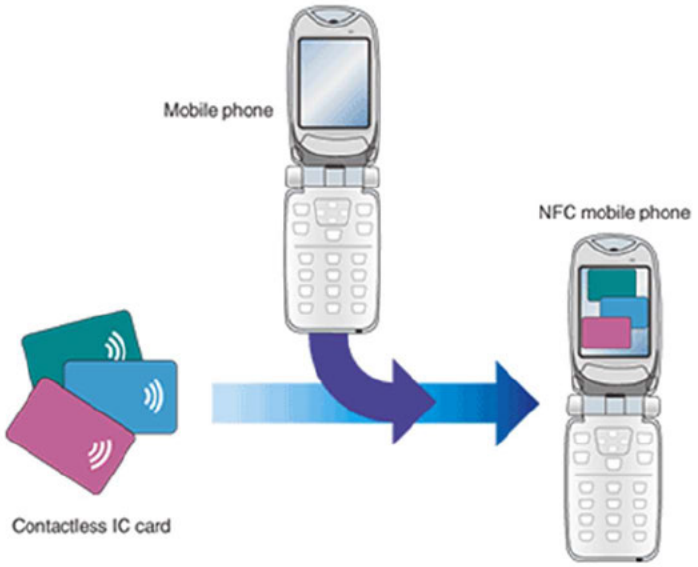

200
204
NFC Sensor Application
202
Mobile Device
206
NFC Component
208
214
Mobile Wallet Application
Processor
218
Mobile Wallet
216
User Interface
210
212
User Action



At 4:40-61, Skowronek discussed, without needing to belabor, that the mobile wallet data could include multiple payment mechanisms or cards:

> In embodiments, the mobile wallet application 306 is software that completes the financial transaction with the NFC sensor application 316 through the NFC application 304. The mobile wallet application 306 can store or extract mobile wallet database 312 from a mobile wallet database 312, which may be stored in a storage medium of the mobile device 302. The mobile wallet database 312 can include information about the user (the user's name, address, phone number, email address, etc.), information about payment types for the user (credit card numbers, expiration dates, stored value accounts, gift card numbers, checking account numbers, other account information), security information (passwords, login credentials, etc.), and/or any other information needed to transact business with the NFC sensor application 316. The mobile wallet application 306 can manage the information in the mobile wallet database 312, allowing the user to add, change, and/or delete the data through the user interface 310. Further, the user may need to login to the mobile wallet application 306 by providing information, for example, a login identification and a password, which the mobile wallet application 306 can compare to the information in the mobile wallet database 312.

Also cited elsewhere in this Background section, an NFC Forum October 2008 whitepaper "Essentials for Successful NFC Mobile Ecosystems" (described and excerpted in Nakamura 2009), graphically illustrated that a single mobile phone could operate as one of several contactless cards:



VI. INVALIDITY UNDER 35 U.S.C. §102 AND §103

A. Anticipation

Samsung contends that the Asserted Claims are invalid as anticipated under 35 U.S.C. § 102 in view of each of the prior art references charted in Exhibits 411-A01-~~A23~~A24, 708-A01-~~A23~~A24, 199-A01-~~A23~~A24, 432-A01-~~A23~~A24, 756-A01-~~A23~~A24, 743-A01-~~A23~~A24, 172-A01-~~A23~~A24, and 793-A01-~~A23:~~A24 (the "A Exhibits"). These A24 exhibits are new with these First Amended Invalidity Contentions. The previously served A01-A23, B, and C exhibits each included multiple recitations of "A01-A23." Each such recitation should now be understood as "A01-A24."

Exhibit No.	Prior Art
-A01	US 2006/0165060 (Dua 060)
-A02	WO 2002/049322 (Holloway 322)
-A03	US 2008/0046366 (Bemmel 366)
-A04	US 2009/0069049 (Jain 049)
-A05	"Kyocera"
-A06	"Nokia"
-A07	"Fujitsu"

-A08	US 9,552,584 (Bierbaum 584)
-A09	US 2009/0144161 (Fisher 161)
-A10	US 9,824,355 (Aabye 355)
-A11	US 10,026,076 (Kumar 076)
-A12	"NFC"
-A13	US 2007/0124211 (Smith 211)
-A14	US 7,478,065 (Ritter 065)
-A15	US 7,992,779 (Phillips 779)
-A16	WO 2006/087503 (Waters 503)
-A17	US 2005/0221798 (Sengupta 798)
-A18	US 2008/0167000 (Wentker 000)
-A19	US 2009/0192935 (Griffin 935)
-A20	US 2010/0082490A1 (Rosenblatt 490)
-A21	Short Range Wireless Technologies with Mobile Payment Systems (Chen 2)
-A22	US 7,058,114 (Dabak 114)
-A23	US 7,962,369 (Rosenberg 369)
-A24	"Motorola"

To the extent any item of prior art cited above is deemed not to disclose, explicitly or inherently, any limitation of an Asserted Claim, Samsung reserves the right to argue that any difference between that prior art and the corresponding patent claim would have been either inherent to the art or obvious to a person of ordinary skill in the art.

Additional prior art has not been charted, but is still relevant to the anticipation of the Asserted Patents, including without limitation as evidence of the state of the art at the alleged time of invention, defining the relevant POSITA, and demonstrating how a POSITA would understand the charted prior art. This includes, for example, prior art identified in Sections IV, V, and VI of these cover pleadings and in the accompanying exhibits. For example, each of the above-identified charts further incorporates by the descriptions of prior art technologies referenced in the above-identified prior art, including the Near-Field Communications ("NFC") standards and related publications (*see* Exhibits 411-A12, 708-A12, 199-A12, 432-A12, 756-A12, 743-A12, 172-A12, 793-A12) and other such technologies (*see* the "B Exhibits": Exhibits 411-B, 708-B, 199-B, 432-B, 756-B, 743-B, 172-B, 793-B).

Samsung reserves the right to amend these Invalidity Contentions to assert these references depending on the infringement positions Telcom may take as the case proceeds and/or on Samsung's ongoing investigation.

B. Obviousness

Each anticipatory prior art reference disclosed in the preceding section as invalidating an Asserted Claim also renders that claim obvious, either alone or in combination with other prior art, as demonstrated in the claim charts appended as the A Exhibits ~~411-A01-A23, 708-A01-A23, 199-A01-A23, 432-A01-A23, 756-A01-A23, 743-A01-A23, 172-A01-A23, and 793-A01-A23~~. To the extent any limitation is deemed not to be exactly met by an item of prior art listed above and in the appended Exhibits, then any purported differences are such that the claimed subject matter as a whole would have been obvious to one skilled in the art at the time of the alleged invention, in view of the state of the art and knowledge of those skilled in the art. The item of prior art would, therefore, render the relevant claims invalid for obviousness under 35 U.S.C. § 103.

In addition, each of the references identified above ~~render~~in this cover pleading renders one or more asserted claims of the Asserted Claims obvious when ~~the references are~~that reference is read in combination with ~~each~~the other references identified above, and/or when it is read in view of the state of the art and knowledge of those skilled in the art. To the extent any of the references in ~~Exhibits 411-A01-A23, 708-A01-A23, 199-A01-A23, 432-A01-A23, 756-A01-A23, 743-A01-A23, 172-A01-A23, and 793-A01-A23~~the A Exhibits is deemed to lack a particular claim limitation, that reference can be combined with the disclosure identified for that limitation in the B Exhibits ~~411-B, 708-B, 199-B, 432-B, 756-B, 743-B, 172-B, and 793-B~~ to render that limitation and Telcom's claims a whole obvious. Samsung may also show that such an allegedly lacking limitation is rendered obvious by the disclosure of any of the other references identified

for that limitation in the A Exhibits ~~411-A01-A23, 708-A01-A23, 199-A01-A23, 432-A01-A23, 756-A01-A23, 743-A01-A23, 172-A01-A23, and 793-A01-A23~~.

Additional prior art, including material referenced herein or produced in conjunction with these Invalidity Contentions, that has not been charted is nonetheless relevant to the obviousness of the Asserted Patents, including without limitation as evidence of the state of the art at the alleged time of invention, defining the relevant POSITA, and demonstrating how a POSITA would understand the charted prior art. This includes prior art identified in Sections IV and V of these cover pleadings and in the accompanying exhibits.

Samsung also reserves the right to amend or supplement these contentions regarding anticipation or the obviousness of the Asserted Claims in view of further information from Telcom, or information discovered during discovery. Telcom has not identified what elements or combinations it alleges were not known to one of ordinary skill in the art at the time. Therefore, for any claim limitation that Telcom alleges is not disclosed in a particular prior art reference, Samsung reserves the right to assert that any such limitation is either inherent in the disclosed reference or obvious to one of ordinary skill in the art at the time in light of the same, or that the limitation is disclosed in another of the references disclosed above and in combination would have rendered the asserted claim obvious.

C. Motivation to Combine

Samsung intends to present expert evidence demonstrating the motivation to combine of one of ordinary skill in the art. Such facts and evidence is expert testimony and will be presented in the experts' reports according to the schedule of the Court. Samsung incorporates by reference its forthcoming expert reports and any testimony of its experts presented according to the Court's schedule. The motivation to combine or modify the above items of prior art are present, for example, in the references themselves, the Asserted Patents, references cited on the face of the

Asserted Patents, the knowledge, skill, or creativity of one of ordinary skill in the art, the prior art as a whole, and/or the nature of the problems allegedly addressed by the Asserted Patents. The law requires no showing of a specific motivation to combine or modify prior art references disclosed herein and in the Invalidity Charts, as each combination or modification of art would have no unexpected results and at most would simply represent a known alternative to one of skill in the art. *See KSR Int'l Co. v. Teleflex, Inc.*, 127 S.Ct. 1727, 1739-40 (2007) (rejecting the Federal Circuit's "rigid" application of the teaching, suggestion, or motivation to combine test, instead espousing an "expansive and flexible" approach). Indeed, the Supreme Court held that a person of ordinary skill in the art is "a person of ordinary creativity, not an automaton" and "in many cases, a person of ordinary skill in the art will be able to fit the teachings of multiple patents together like pieces of a puzzle." *Id*. at 1742. Thus, to a person of ordinary skill in the art, the Asserted Claims represent solutions that would have been obvious to try, with predictable results.

Nevertheless, should additional evidence of motivation to combine or modify be required to render the Asserted Claims obvious, Samsung contends that there was a motivation to combine the references identified above. That motivation was provided in the nature of the problem allegedly solved by the Asserted Patents, the teachings of the cited prior art itself, and/or the knowledge of a person of ordinary skill in the art. For example, the combinations identified above would have been combined or modified using: known methods to yield predictable results; common sense; known techniques in the same way; a simple substitution of one known, equivalent element for another to obtain predictable results; and/or a teaching, suggestion, or motivation in the prior art generally. In addition, it would have been obvious to try combining or modifying the prior art references identified above because there were only a finite number of predictable solutions and/or because known work in one field of endeavor prompted variations based on

predictable design incentives and/or market forces either in the same field or a different one. In addition, the combination of the prior art references would have been obvious because the combination represents known potential options with a reasonable expectation of success.

Additional evidence that there would have been a motivation to combine or modify the prior art references above includes the interrelated teachings of multiple prior art references; the effects of demands known to the design community or present in the marketplace; the existence of a known problem for which there was an obvious solution encompassed by the Asserted Claims; the existence of a known need or problem in the field of the endeavor at the time of the alleged invention(s); and the background knowledge, skill, or creativity that would have been possessed by a person having ordinary skill in the art. Samsung may rely on uncited portions of the prior art references cited and produced, other publications and testimony, and the testimony of experts to establish that a person of ordinary skill in the art would have been motivated to modify or combine certain of the cited references so as to render the claims obvious.

For example, where multiple publications describe the same system, describe devices that are intended to be used together, or are from the same author, publisher, or manufacturer, one of ordinary skill would be motivated and find it obvious to read those publications together and combine their disclosure. As another example, where a product was available in another country, the availability of such a product would motivate a person of ordinary skill to arrive at the same or similar product in the United States. As yet another example, where the prior art identifies the desirability of or plans for future enhancements of a system, a person of ordinary would be motivated to incorporate such enhancements even if the original developer or author was unable to complete those enhancements.

References identified by Samsung relate to the same technological and commercial field as each other and the Asserted Patents. The common specification defined the "field of the invention" as "systems, devices and/or methods that may be used to provide an adaptive enablement of one or more communications modes based upon having satisfied a proximity criterion." '411 patent at 1:5-12. The common specification admits that "those skilled in the art will appreciate" that a "communications device may be configured to estimate its location and the value of 'at least one other parameter' by, for example, processing GPS signals and/or by using other means and/or sensors that may, according to some embodiments, be device-based and/or network assisted/based means and/or sensors." *Id*., 6:9-16. Included, therefore, in the field of invention are those references that are or relate to the mobile wireless devices, communication modes used by those devices, sensors of all varieties that could be used by mobile wireless devices or whose inputs could be processed and conveyed to such devices, and securing or adapting features and communication modes based on data or processed data from such sensors. This includes, for example, art related to fingerprint, retina, and other biometric sensors; proximity and location sensors and approximators; cellular, Wi-Fi, Bluetooth, RFID, IrDA, NFC and other communications protocols; and systems for proximity-based contactless payment, including those that leveraged any of the previously recited protocols. All of the prior art identified by Samsung is within this field.

References identified by Samsung address the same technical issues and suggest very similar solutions to those issues discussed in the Asserted Patents and generally known at the time of the alleged invention(s) claimed in the Asserted Claims. As explained earlier in these Invalidity Contentions, the common specification purports to be directed to the alleged "rigidity aspect that is associated with wireless mobile devices in that a wireless mobile device is typically configured

to be capable of performing a predetermined number of functions independent of its location, Time-of-Day (ToD), velocity, acceleration, temperature, sensing of a signal, etc." 1:20-25. According to the specification, "[i]t would, for example, be desirable to have a mobile wireless device act as a 'wallet' (over and above other functions) only when it is time to pay for an item and not act as a wallet when there is no need to do so." 1:25-28. The disclosed and claimed solutions generally involve some combination of one or more of (1) enabling a wireless device to have wallet functionality, perhaps contingent on a biometric input, (2) allowing a wireless device to engage in a transaction, perhaps contingent on a biometric input and the device being proximate to a payment point, and (3) performing that transaction. Many of the prior art references that Samsung cites in these Invalidity Contentions address the same so-called problem. For example, contactless payment systems, whether via smartcards or mobile phones (both wireless devices), typically involved an initial provisioning of payment functionality (e.g., charging the wireless device with funds, downloading payment account information to the device, or enabling payment software on the device) and called for a per-transaction pre-transaction process (e.g., proximity to the point of payment, biometric sensor, presentation of corroborating information to the merchant or point of sale system, etc.). Prior art references also describe the history and value of this paradigm, which is at least as old as the use of a letter of credit, including in the context of payment cards (e.g., credit, debit, and gift), and contactless payment (e.g., via fob, smartcard, and mobile phone).

References identified by Samsung disclose software capable of being implemented on existing hardware, and/or existing hardware capable of being integrated with existing hardware, both yielding predictable results. For example, as evidenced by the actual release of mass-market mobile phones supporting multiple communication means (e.g., cellular and one or more of

Bluetooth, Wi-Fi, IrDA, and NFC/RFID), integrating those technologies and software for controlling and applying those technologies was within the abilities of one of ordinary skill in the art. Similarly, and also as set forth elsewhere in these Invalidity Contentions, it was already known that biometric sensors such as fingerprint sensors could be implemented on mobile wireless devices to obtain the expected result.

Additional motivation to incorporate any of the concepts claimed in the Asserted Claims of the Asserted Patents into any primary reference allegedly missing those concepts is set forth below.

A person of ordinary skill in the art would have had additional motivation to use RFID, NFC, or Bluetooth as the means of communication between a wireless mobile device and a point of sale payment terminal. As set forth in the Background section and elsewhere in these Invalidity Contentions, by the beginning of 2008 there were dozens of wide-scale and well-publicized uses of NFC-enabled phones for contactless point of sale payments, including nation-wide deployments in Japan and South Korea and multiple trials in the United States. NFC was affordable, proven, and standardized. Less ubiquitous, but widely referenced in the literature at the time, was using Bluetooth for these purposes. Industry associations like the Smart Card Alliance had listed it side-by-side with NFC/RFID as a viable means of connecting wireless devices with point of sale systems, and it was disclosed for those purposes in several patents.

Additional motivation to combine mobile phones, and in particular smartphones, with contactless payment technology can similarly be found in the actual success of such systems. A person of ordinary skill in the art at the time could scarcely avoid hearing about the successful use of mobile phones with contactless payment services around the world, and would have been aware of the numerous trials taking place in the United States, including those documented herein. Such

a person also would have been aware that phones with NFC connectivity were being announced and released around the world. Even before the release of the first iPhone and the first Android-powered mobile phone, both of which would have been known to one of ordinary skill in the art, powerful smartphones existed and multi-function PDAs included cellular connectivity. Many of these developments are identified in the Background section, above. The popularity, additional power, and fundamental similarity of these devices as compared to more traditional mobile phones would all motivate one of ordinary skill to combine them with contactless payment systems.

Motivation to combine mobile phones with contactless payment systems could be found across the industry. As set forth in references cited in the Background section and elsewhere in these Invalidity Contentions, it was known that customers in the United States and around the world appreciated the speed and convenience of contactless payments. It was also known that consumers liked the additional convenience of not having to fish a card from a wallet or purse, or being unable to pay if they forgot their wallet or purse. Credit card companies and banks had an interest in increasing the use of contactless payment system, and enabling mobile phones to work with their existing and growing systems would do that. Moreover, merchants involved in contactless and mobile phone payment trials were reporting that the increased convenience was resulting in increased sales. Mobile phone companies and mobile network operators, meanwhile, were interested in increasing the value proposition of their phones and (at a time when many phones were specific to a network operator) the phones available on their network. This broad-based interest in the convergence of mobile phones and contactless payment is evidenced by the cross-industry membership of the NFC Forum and Smart Card Alliance, both of which were active in supporting such efforts. It is also evidenced by the diversity of companies whose employees sought for or obtained patents in area of contactless payments, including American Express,

MasterCard, Visa, Motorola, Nokia, Ericsson, Sony, Fujitsu, PayPal, ViVOtech, First Data, T-Mobile, Vodafone, and others.

Security and authentication go hand-in-glove with commerce and payment. Even before the advent of contactless payments, credit card companies had a vested interest in making sure that credit cards were enabled or activated. For example, in 1958, Bank Of America mass mailed pre-approved credit cards in "the Fresno drop", resulting in higher than expected fraud rates. *See, e.g.*, https://yaspahq.medium.com/a-history-of-the-payments-industry-part-1-8cee936105b9. Customers, merchants, and credit card companies, and banks have long had a similar interest in authentication and preventing lost or stolen credit cards from being used by others or in excess of their allowed limits. Multiple points of enablement, authorization, or authentication were known and of interest. These include enabling a card or payment mechanism, enabling it for use on a mobile device, allowing access to a payment application on a mobile device, and conducting an actual transaction. Just as contactless payment systems made bona fide use more convenient and efficient, it also had the potential to make abuse more convenient and efficient. Because one of the advantages of contactless payment is convenience and speed, it was not desirable to encumber the payment process with manual phone calls or photo-identity checks to confirm that the possessor of the contactless device was an authorized user. Similar concerns applied when associated a card or account with a contactless fob, a digital wallet, or a mobile phone: was that association being created by someone authorized to do so. The use of biometrics to answer this question was an obvious solution. Another oft-considered scenario was theft, which raised the question of how to confirm that the possessor of a contactless payment device allowed to use it. One solution was require authentication when the contactless payment device or wallet was activated, and then to have it timeout or otherwise deactivate a reasonable time later (such as when it was no longer

within range of a payment terminal). Another approach was to require authentication on a per-transaction basis, either before connecting to a point of sale system or before confirming that payment should be made. At all of these stages, biometric authentication was an obvious and well known solution, with fingerprint sensors already available for use in mobile devices, including phones, as described above in the Background section. Moreover, it would have been obvious to one of ordinary skill in the art to combine disclosures of various authentication, activation, and enablement protocols with each other and with disclosures of payment systems, for at least the reasons set forth in this paragraph.

Amplifying what is said above in the exhibits about, *e.g.*, the Kyocera devices demonstrated at CTIA 2008 and used in the May 2007 Cellular South trial, before the alleged invention of the Patents-in-Suit, Atrua had developed, offered for sale, and sold fingerprint sensors for the precise purpose of integration with smartphones. Such a sensor was used in the Kyocera smartphone that was part of the Cellular South trial: Atrua Made-For-Mobile Fingerprint Solution Enables First-Of-Its-King Mobile Commerce Trial in U.S., Atrua Technologies, Inc., https://web.archive.org/web/20071113002541/http://atrua.com:80/press_release_10-22-2007.html (Oct. 22, 2007). Altrua first announced those devices at least as early as 2006. *See, e.g.*, https://web.archive.org/web/20071113002541/http://atrua.com/press_release_10-22-2007.html; https://web.archive.org/web/20070617054437/http://www.atrua.com/s-mobilephones.html; https://web.archive.org/web/20060208013501/http://atrua.com/solutions_all.html; https://web.archive.org/web/20060324011604/http://www.atrua.com/p-wings.html; https://web.archive.org/web/20070806153511/http://www.atrua.com/press_release_03-26-2007.html; https://web.archive.org/web/20081026014044/http://www.atrua.com:80/news.html. Authentec, a rival to Autra, also sold fingerprint sensors used in many mobile phones in the

relevant time period. *See, e.g.*, https://web.archive.org/web/20080703230624/http://authentec.com/products-wireless-aes1710.html; https://web.archive.org/web/20080703230509/http://authentec.com/customers-wireless.html; and https://web.archive.org/web/20070701022823/http://www.authentec.com/news-item.cfm?newsID=200.

Proximity-based activation of contactless payment methods was similarly an obvious and logical feature of electronic payments and wallets. Just as one does not publicly circulate one's credit card number, it was desirable for a contactless payment system to share payment details only with authorized terminals and not with the world at large or with illicit eavesdroppers. In addition to encryption, a common-sense and widely adopted approach, as documented it the Background section and elsewhere in these Invalidity Contentions, was to use short-range wireless signals for that communication: IrDA, Bluetooth, and RFID/NFC. The technical details of how RFID works means that it can be inherently limited to operate only when an RFID transmitter is very close (a few inches) from an RFID reader—and, for mobile devices, only when the RFID transmitter is active. Other communication modalities have similar limitations, and those of ordinary skill in the art had at their disposal a variety of others ways to determine the location of a wireless payment device and its proximity to a point of payment. In order to reduce the chances of a wireless payment device broadcasting payment information, a person of ordinary skill in the art would have been motivated to combine proximity detection with contactless payment systems—and, indeed, that was a prime focus of NFC and numerous publications and systems publicly known prior to the alleged invention of the Patents-in-Suit, as explained above.

These concerns about ensuring that payment information is secure and is used only by authorized users would also motivate one of ordinary skill in the art to look more broadly to art relating to selectively enabling or disabling functionality on a mobile phone. In the context of contactless payments, a specific concern was to prevent an unauthorized user from accessing and using the functionality that would allow them to make payments. Even in scenarios where a user was authorized to access some functionality of the device, a separate access privilege might be associated with the payment functionality. This type of concern existed independently of contactless payment systems. For example, it was desirable to allow a mobile phone to be used to make emergency phone calls, but to require additional authentication to access other features. And even if a phone was otherwise accessible, high value features or functionality might need separate authentication. Also, certain functionality might be selectively enabled based on the presence or absence of certain network connections. In the interests of improving the security of contactless payment systems, a person of ordinary skill in the art would have looked to and leveraged disclosures and developments in these and similar areas.

One of the early-recognized advantages of using a wireless device for contactless payment was that it could replace the myriad physical cards crammed into a user's physical wallet. Some of the prior art references do not recite the use of multiple cards, but a person of ordinary skill would have done so using their own common sense and/or by combining those references with others that disclose multi-card systems. Those references sometimes adopted the "digital wallet" approach, whereby a specific software application on the wireless device contained the details of the various cards. Sometimes it was through this digital wallet that authorization to use the cards was obtained and secured, and sometimes it was this digital wallet that needed to be enabled before a contactless payment could be made. Sometimes these digital wallets were implemented in

software, in hardware, or in a combination of the two. Some of these approaches are presented in references discussed in the Background section. Others are presented in the invalidity charts. A person of ordinary skill in the art would have been motivated to combine multi-card functionality, including but not limited to as disclosed with digital wallets, with contactless payment systems.

It would also have been obvious to one of ordinary skill in the art to combine any of the references that disclose mobile phones, wireless communications, or cellular communications with OFDM or OFDMA. As set forth in the Background section, above, OFDM and OFDMA were used in Wi-Fi and WiMax standards, both of which were already supported by commercially available mobile devices. It was also known in early 2008 that upcoming 4G cellular networks would use OFDMA.

Certain of the Asserted Claims recite limitations related to both enabling some functions and disabling other functions in response to a condition being met. One of ordinary skill in the art at the time would have known that mobile devices had long-support lock and unlock modes and increasingly supported elevated security or authentication for specific applications or data. Given the sensitive nature of payment-related information and the potential value of transactional functionality, a person of ordinary skill in the art at the time would have tried, with a reasonable expectation of success, various combinations of disabling and enabling lock modes, disabling and enabling communication interfaces, and disabling and enabling applications (for example) in response to conditions such as attempted or successful biometric authentication. Different approaches could all be implemented with a reasonable certainty of success, and would be implemented to, for example, achieve different balances of usability, security, flexibility, and convenience.

A person of ordinary skill in the art at the time would also have understood that references disclosing an integral point of sale terminal with the ability to conduct short-range transactions (proximity payments) could be modified to be multiple physically distinct separate components, such as a separate short-range reader and a traditional point of sale terminal. For example, the person of ordinary skill in the art would have been aware that vendors like ViVOtech (including vendors mentioned in the Background section in the context of contactless payment trials and those mentioned in, e.g., the Smart Card Alliance's February 2007 publication "Contactless Payments: Frequently Asked Questions.") offered both configurations and with no material change in relevant functionality.

Various of the references cited herein (including in the invalidity charts) disclose reporting and management that is associated with or facilitated by mobile phone payment systems and their increased use. Mobile phone payment systems have the potential to generate more data in more structured ways than (for example) cash transactions or card payments. The literature and common sense suggest numerous such scenarios, including reporting transaction information to loyalty card systems, to vendors or supply chain management systems, to risk management systems, to contacts such as family or friends, to reimbursement or expense reporting systems, and the like. Moreover this information could be sent over a variety of communication protocols, depending on the nature of the report and the nature of the system receiving the information. One example of this type of message flow is disclosed in US20050222961A1 (Staib). Staib describes a scenario in which a mobile device is associated with one contactless payment system and can emulate other payment systems. [0022]. After a transaction takes place, an ensuing message flow coordinates the various systems involved in the emulation. [0023]. Staib also describes a potential consequence of payments systems that allow transactions to take place without waiting for back-end systems to

confirm that the payment should be allowed. See, e.g., [0060]. This approach was a common one that balanced convenience against risk. Staib explains that in some implementations of such a system, something (e.g., the merchant's point of sale system or the user's mobile phone and wallet software) has to report the details of those transactions to an actual back-end system for settlement. [0060]. A person of ordinary skill in the art would have been motivated to combine this knowledge and common sense to any of the references or combinations of references disclosing contactless payment systems, augmenting those payment systems to include additional communications and message flow to provide alerts and reports to end users, service providers, and interested third parties like those discussed herein.

A person of ordinary skill in the art would also have combined teachings related to over the air authorization and teachings related to digital wallets with references and combinations that disclose contactless payment systems. For example, and as presented in references cited in the Background section, allowing a user to OTA register a mobile phone with a payment mechanism such as a credit card or debit card provided flexibility and value users were able to access more of those mechanisms via the phone, to payment mechanism providers for whom it increased the potential user base, and even for phone and mobile service providers who did not have to pre-load information onto SIM cards or into mobile phones. Digital wallets, in addition to having their own independent benefits, complemented OTA enrollment. The wallets allowed users to add, modify, and access the various payment mechanisms (e.g., their different credit and debit cards) associated with their phone, regardless of that associated was created. But the wallets could also provide additional security to the OTA process (e.g., if the wallet itself required biometric or other authentication). And wallets or wallet providers could serve as an OTA service provider, leveraging their own capabilities to provide that functionality on behalf of card issuers who did

not have their own OTA facilities. A person of ordinary skill in the art at the time would thus have had numerous reasons to combine both digital wallets and OTA enrollment with contactless payment systems.

Certain of the Asserted Claims recite repeating a set of steps. For example, some recite repeated sensing of parameters. Others recite repeating an a transaction enablement process or a transaction performance process. A person of ordinary skill in the art would have known that software and hardware that could perform these things once could perform them repeatedly, and would have recognized the value in doing so. For example, confirming a user's identity a single time is useful, but it can also be useful to do so repeatedly (e.g., to confirm that an application should remain open/closed or a functionality should remain enabled/disabled). Reinforcing what is set forth in the preceding paragraph, a person of ordinary skill in the art would also have known that repeating a card enrollment process (for example) allows for a mobile phone to be associated with multiple cards, and that repeating a transaction process allows a user to make multiple purchases.

D. Simultaneous "Invention" By Others

As evidenced by the material presented in the Background section and the invalidity charts, the subject matter of the Asserted Patents was being (indeed, had been) actively explored by others at the time of alleged invention. The world-wide cross-industry activity in this field, loosely characterized as mobile payments, is its own motivation to combine the various cited references: a person of ordinary skill in the art at the time would have been aware of work done by credit card companies and banks, point-of-sale vendors, mobile phone vendors and network operators, settlement companies, smartcard manufacturers, and component suppliers. Such a person would also have been aware of the many standardization efforts, analyst reports, whitepapers, customer trials, and actual deployments.

The breadth of this activity is itself indicative of obviousness, as Samsung will more fully explain at the appropriate time in accordance with the schedule set by the Court.

In addition to what is cited above and in the exhibits to these Invalidity Contentions, additional evidence of simultaneous invention by others includes the following.

In 2004's "Short-range wireless technologies with mobile payments systems," Chen and Adams review short-range wireless technologies from the perspective of mobile payments. They provide an overview of Bluetooth, noting its affordable implementation, use of the unlicensed ISM band, relatively short range, and commercial use. (p. 650). They do the same for infrared/IrDA, RFID, and NFC (pp. 650-51), include this summary at 651, and discuss other aspects of each of the protocols from the context of mobile payments systems (pp. 651-52).

	Standard	Throughput	Range	Radio frequency	Price	Power consumptions	Key players	Application areas
Infrared	IrDA	1.152 kbps – 4 mbps	1 - 5 meters	(Infrared light)	$2	Very low	Agilent, Microsoft Motorola and Sony Ericsson Mobile	Data exchange, devices remote control, payment systems.
Bluetooth	IEEE 802.15.1	720 Kbps– 1 Mbps	10-100 meters	2.45 GHz	$5	Low	Ericsson, IBM, Intel, Nokia Toshiba	Data exchange, electronic devices remote control, payment systems.
RFID	ISO/IEC 14443	4-128 Kbps	10 feet	120-140 KHz	$3-$10	Very low	Honeywell, Texas and Philips	Access control Inventory control
RFID			10 feet	13.56 MHz	$0.5 - $5			Access control Smart cards
RFID			40 feet	869-956 MHz	$0.75			Railroad car monitoring, Toll collection systems
NFC	ECMA 340, ISO/IEC 18092	424 Kbps	Up to 20 cm	13.56MHz	20 cents	Very low	Philips & Sony	Data exchange, contact less smart card

Table 1. Main characteristic of wireless technologies

They discuss two existing mobile payments systems, one involving IrDA and one involving Bluetooth (pp. 652-53), and conclude by identifying the value of further work with respect to business models, interoperability, security implementations, availability, and reliability (p. 653).

In "The economics of mobile payments: Understanding stakeholder issues for an emerging financial technology application" ("Au and Kauffman"), published in January 2007, the authors

observed that with respect to mobile payments, "[t]wo technology standards, among others, are helping to achieve device and platform interoperability, resulting in current projections for high growth. They are short message services (SMS) and near field communications (NFC)." Page 141. With respect to NFC in particular, they noted that: "NFC is used by VIVOtech (www.vivotech.com), which partners with companies such as Phillips, American Express, MasterCard, Visa, Symbian, and Sprint, and MobileLime (www.mobilelime.com), which partners with IBM, Chase, Fujitsu, HSBC, and Verifone, among others." (Page 142). The vast range of global developments, supported by multiple citations, was summarized: "Depending on where an observer looks in the world, the extent of interest and the degree of development and diffusion of m-payments systems and alternative electronic cash systems will dramatically differ. Many of the European countries, and Korea, Singapore and Japan have already gone far down the path of technological innovation, systems design, implementation, adoption, use and refinements. The United States is farther behind. Many researchers and business analysts believe that m-payments will flourish in the coming years as the underlying technologies and the market for digital wireless phones mature. Even today, m-payment technologies already look promising, since they seem to be so well attuned to consumer needs. A recent usability study conducted by Royal Philips Electronics and Visa International on NFC protocols and contactless payment technology shows that consumers like the convenience and ease of use for transactions and payments with their mobile phones. As a result, the market for m-payments seems to be growing rapidly—indeed, the market is in ''takeoff'' mode. Celent, a research and consulting firm, projects that worldwide mobile payments have reached US$24 billion in 2006 and more than double to US$55 billion by 2008." (Page 142, citations and footnotes omitted.) The paper went on to analyze global efforts and their economic contexts.

Pasquet and colleagues wrote several papers after an NFC-payments trial in Strasbourg, France that had started in November 2006. E.g., "Secure Payment with NFC Mobile Phone in the SmartTouch Project" and "Payment with mobile NFC Phones: How to Analyze the Security Problems." They described the trial as involving an "NFC-based payment application that fully supports the international EMV standard and the [MasterCard and Visa] PayPass program." Secure Payments at 121. They noted that by 2007, there were at least 2 million contactless MasterCard and Visa card issued in the United States and another million in Europe. *Id*. They described a test deployment that used off-the-shelf components that implemented international standards. *Id*. at 121-22. The relevant standards and technologies were sufficiently well understood that the paper needed to only briefly review them and describe what options had been selected for this particular implementation. *Id*. at 122-23.

There was sufficient *academic* work in the field that in February 2007, Dahlberg and colleagues published "Past, present and future of mobile payments research: A literature review," citing approximately 70 peer-revied academic papers. The authors described the basics of a mobile payment and spoke about the volume of activity at page 166:

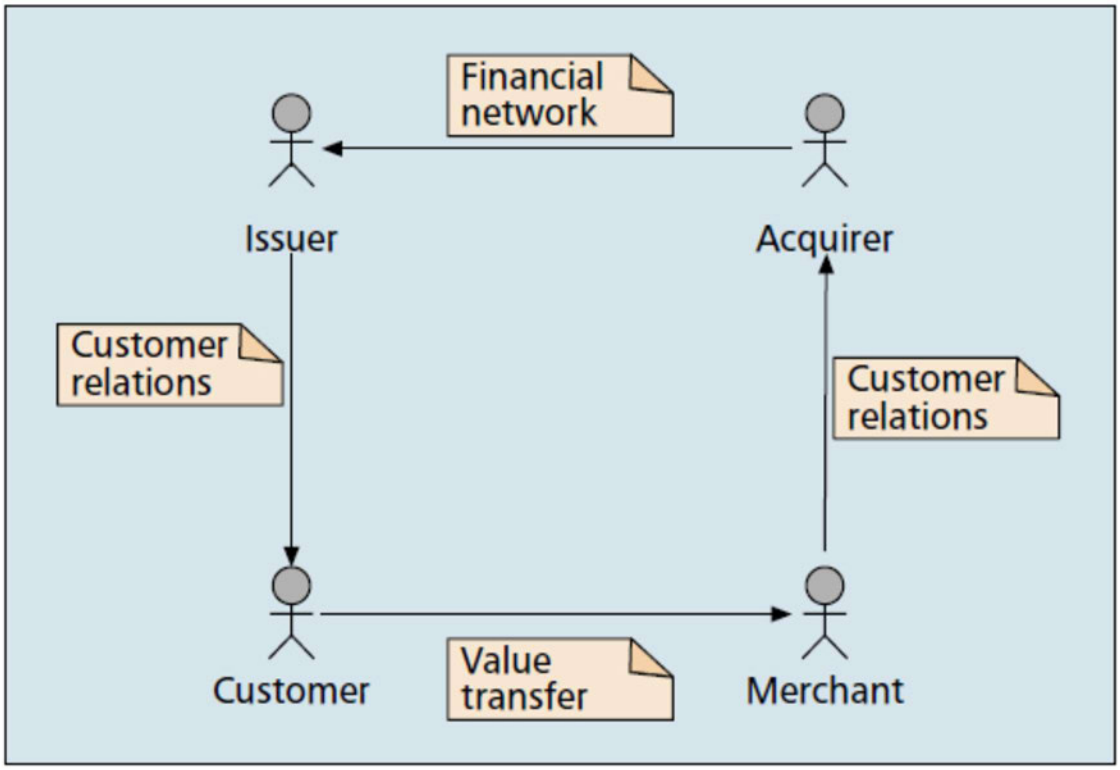
> A mobile payment is carried out with a mobile payment instrument such a mobile credit card or a mobile wallet. In addition to pure mobile payment instruments, most electronic and many physical payment instruments have been mobilized. Furthermore, mobile payments, as all other payments, fall broadly into two categories: payments for daily purchases, and payments of bills (credited payments). For purchases, mobile payments complement or compete with cash, cheques, credit cards, and debit cards. For bills, mobile payments typically provide access to account-based paymen t instruments such as money transfers, Internet banking payments, direct debit assignments, or electronic invoice acceptance. In the early 2000s, mobile payment services became a hot topic and remained so even after the burst of the Internet hype. Hundreds of mobile payment services, including access to electronic payments and Internet banking, were introduced all over the world.

The authors commented on the diverse competitive pressures at play (pages 166-67) and noted the tight restrictions they imposed that excluded certain research in the field of mobile

payments and that excluded all research not explicitly directed to mobile payment services (pages 167-68).

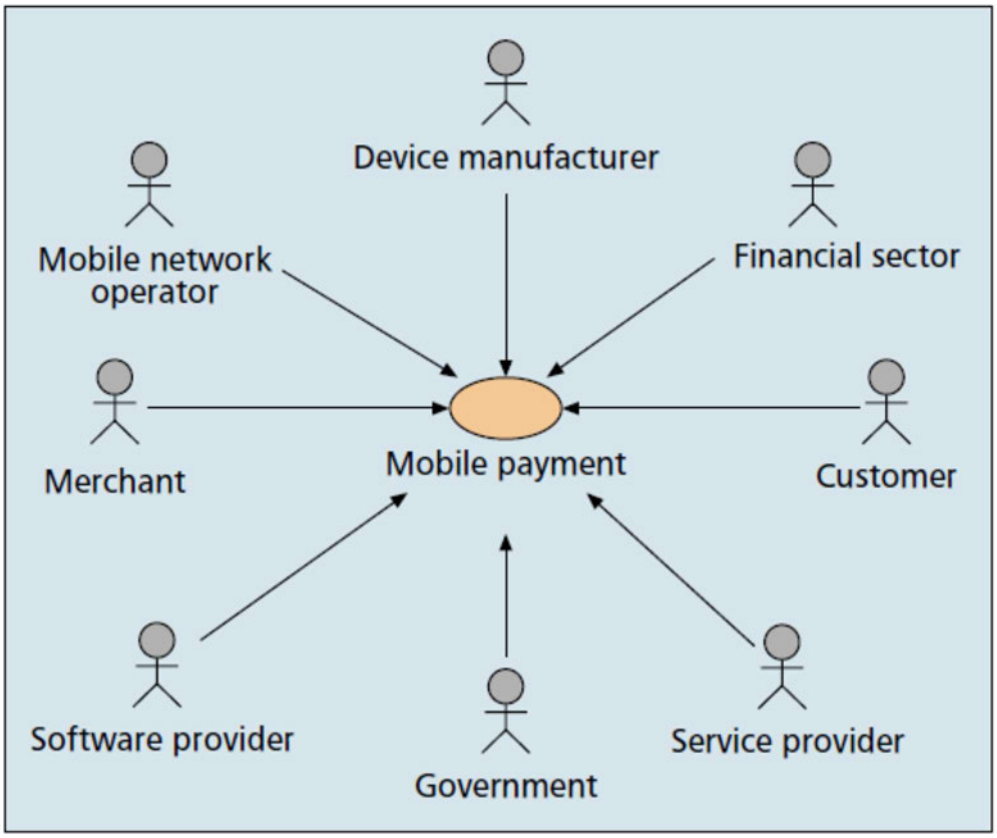
Nearly three years *earlier*, in October 2004, Karnouskos had published "Mobile payment: A journey through existing procedures and standardization initiatives." This was a more pragmatic survey of the field: "in this article we will provide an overview of the mobile payment area, focusing on standardization consortia that have emerged … as well as the existing mobile payment services that have been launched. … The motivation is to provide a handy overview of past and existing efforts in the domain, which can be used as a starting point by those interested in this exciting area. We have also tried to refer to projects all over the world, including the Internet URLs of the companies or the projects that have participated, as well as a bibliography that one can follow in order to acquire further technical and conceptual details." (p. 45).

Karnouskos observed that mobile payments are "possible on virtually any mobile device, including: A tablet PC (which is a full-function PC with limited mobility, usually used by one person). A PDA (a truly mobile device with multimedia and connectivity capabilities). A smartphone (a consolidation of PDAs and legacy mobile phones). Any mobile payment terminal or device (merchant-operated terminals with built-in security) capable of initiating, activating, and/or confirming a payment." (p. 44). He illustrated and described a "typical digital payment scenario" on page 45:



The customer is the party making the payment; the merchant is the party accepting the payment; the acquirer is the third party that has a relationship and interacts with the merchant; and the issuer is a third party that has a relationship and interacts with the customer. In any transaction the goal is the value transfer from the customer to the merchant. A typical procedure followed by credit card companies is as follows. The customer "pays" a merchant for goods/services. Subsequently, the merchant sends the transaction details to the acquirer for clearing. The acquirer sends the transaction details to the financial network to which it belongs (e.g. VISA) which then forwards the details to the issuer. The issuer is informed to make the necessary fund reservation at the customer side. The scheme settles/pays the acquirer, the acquirer settles/pays the merchant, the issuer settles/pays the scheme, and the customer pays the issuer. However, other schemes may directly exchange tokens (e.g. cash, e-tokens) between the customer and the merchant. In the mobile payment arena we have similar procedures, with the only difference being that the customer and possibly the merchant use mobile devices in order to realize a transaction.

The article also identified the diversity of participants in the mobile payment space, including via this figure on page 45, which was discussed on pages 45 and 46, emphasizing the reality of and the need for cooperation within and among categories of participants.



On pages 46 and 47, he discussed some of the well-known features that would be valued in a mobile payment system, including: simplicity and usability (including "the ability to highly personalize the service in order to easily integrate it to [the customer's] everyday payment activities"), universality (applicable to all payment scenarios), interoperability ("interconnection of networks and systems… based on standards and open technologies"), security/trust/privacy ("all steps should be secured/trusted from a technological as well as social perspective"), cost, speed, and "integration of legacy approaches." Notably, the recognized need for these features would have motivated a person of ordinary skill in the art to look to art from these fields and directed to these issues.

On pages 48 and 49, Karnouskos provides an explanation of the conditions that were driving interest in mobile payments. He pointed to the high penetration rate of mobile phones and their transformation "into personal trusted devices that most people carry around with them all the

time." "They are always on and enable direct contact with the owner. This simply means that via mobile phones anyone is reachable anytime, anywhere, which fits perfectly into the vision of a mobile future.." He observed that mobile network operators were regularly deploying new infrastructure and the mobile devices were iterating and improving rapidly. He also observed that mobile phones "can deploy state of the art security (and are expected to do more in the future, e.g. integrate biometric features)" and are inherently linked to a user. He then highlighted research reports that predicted "118 million Europeans, 145 million Asians, and 22 million Americans intend to use their mobile phone to pay for small purchases," "in 2002 that the volume of mobile business will reach $225 billion by 2005," "global m-payment transaction revenues will increase from $3.2 billion in 2003 to $11.7 billion in 2005 and $37.1 billion in 2008," "the size of the mobile Internet-based mobile payment market will grow from around €5 billion in 2002 to nearly €55 billion in 2006," "forty-four percent of 5,600 mobile phone users on four continents surveyed .. would like to use their mobile phones for small cash transactions," and "global mobile commerce is predicted … to attract 1.7 billion users in 2008, who will use their mobile phone handsets to make an anticipated $554 billion in transactions."

One of the types of mobile payments described was "Proximity/Local Transactions": "transactions where the mobile device locally communicates (e.g., via Bluetooth, IrDA, RF, Near Field Communication) with a POS/ATM, e.g. payments at unattended machines, mParking, payments at traditional POS, or money withdrawals from a bank's ATM." (p. 49). On pages 50 and 51, he identified various implementation approaches, including wireless wallets ("a payment application is placed in the mobile phone of the user with all of his data entered once (and not on every transaction), which allows the customer to make mobile payments."), IrFM-based ("based on the IrFM Point and Pay profile standard of IrDA" and "more popular in Japan and Korea, but

there have also been trials in the U.S.") and RFID-based or contactless chip cards (aimed at "smooth migration of existing infrastructure. A contactless chip or a RF-ID tag on the mobile side … is combined with a user authorization on POS (PIN entry). In this way the consumers just have to place the phone close to the POS or ATM in order to initiate the payment."). With respect to RFID payment, he noted that "Nokia/MasterCard, QuickWave, and ExpressPay are some examples in this category."

As stated on page 51, "interest in MP is evident, the standardization efforts are ongoing, and the search for the right business models as well as the successful approaches is ongoing. … the area is active and of great interest…" Page 52 included a list of dozes of mobile payment solutions then on the market, from which the paper segues into a discussion of what is on the immediate horizon. Karnouskos highlights developments in Japan, noting that "Fujitsu's F900iC 3G handset not only supports the mobile wallet function available to the 46.6 million customers of NTT DoCoMo, but also can be locked and accessed securely via a fingerprint scanner." (p. 54.) As to NFC more generally, the article says the following on page 54:

> As NFC is an open standardized platform technology, it is interesting to deploy it in several MP scenarios and develop secure "touch and pay" approaches. Contrary to RFID, where usually the tags are mobile and the readers are stationary, NFC supports exactly the opposite, more interesting model, where the tags are stationary and the readers are mobile. NFC allows reading a tag only when it is pressed against the phone, therefore eliminating the possibility of accidental scanning and preserving valuable system resources such as battery life, which will remain a limiting factor, at least until fuel cell-powered mobile phones become a commodity. Adopting NFC-based MP will mean that the device can authenticate on behalf of the user, which will eliminate the need for PIN numbers and passwords, and boost user friendliness. According to a recent ABI Research study [25], handsets with embedded NFC chips will be available in 2005, and exceed 50 percent of market share by 2009. The open question that remains is what happens if the phone gets stolen, but as VISA points out, this is no different than loosing [sic] a credit card today.

Returning to simultaneous invention, the article concludes with an 11 page appendix briefly describing over 30 standardization and "influential" consortia and more than 100 mobile-payment

deployments or initiatives. To be clear, this includes only a brief mention of the Japanese mobile payment efforts that went live around the time the article was published and only one of the NFC payment trials mentioned above, most of which began approximately a year after the article was published.

A few months later, Dewan (of First Data Corporation) and Chen published "Mobile Payment Adoption in the US: A Cross-Industry, Crossplatform Solution." They defined mobile payment as "making payments using mobile devices including wireless handsets, personal digital assistants (PDA), radio frequency (RF) devices, and near field communication (NFC) based devices" and noted that "[r]esearch and development efforts from financial and technology firms to develop mPayment methods have given rise to a myriad of incompatible and competing standards. According to ePayment Systems Observatory's database (http://www.e-pso.info/), over 183 types of mPayment systems exist just within Europe." (page 2). This was because "the payment industry is experiencing a convergence of technologies and transaction processes. Recognizable benefits for stakeholders and changing consumer behaviors that favor adopting new and creative forms of payment methods are witnessed around the world." (*Id.*)

After reviewing two types of mobile payments (cellular and contactless) and discussing varieties of contactless including RFID and NFC, the article reviewed contactless mobile payment solutions including SK Telecom's MONETA (launched in 2001, with over-the-air card authorization planned) and MasterCard PayPass ("By the end of 2004, approximately 50,000 PayPass cards, stickers, and cell phone covers had been produced. Issuers are following a geographic centric issuance strategy with initial deployments in Dallas, Orlando, and New York."). It then outlined the authors' view of what a nationwide US system might look like, noting (on page 21) the need for cooperation and standardization across a variety of entities:

This model will require a cross-industry cross-platform implementation of the following value chain:

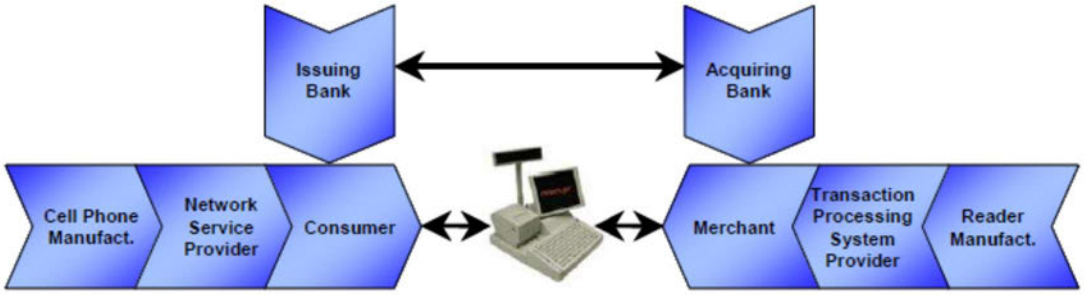


Figure 1. mPayment Value Chain

A 2006 publication from GlobalPlatform described two mobile contactless payment solutions using its technology. Concise Guide to Worldwide Implementation of GlobalPlatform Technology. On page 3, it described the SK Telecom Moneta deployment:

> In 2004, Singapore based Cassis International launched its MobileMatrix solution that enables customers of SK Telecom, the #1 mobile phone service provider in South Korea, to download a credit application onto the SIM over-the-air. It's the world's first over-the-air download of an EMV payment application onto a USIM enabled 3G phone. The SIM card communicates with SK Telecom's back-office network and sends commands to drive the handset, allowing the mobile phone to act like a credit card. Customers can use the downloaded applications to make purchases with their phones via infrared waves or radio frequencies at point-of-sale terminals equipped with dongles to accept the transmissions. … SK Telecom customers can decide the type of applications to be loaded into their handset, which include CAS (Conditional Access System) for DMB (Digital Multimedia Broadcasting through satellite) and T-Money (Public Transportation).

E. No Secondary or Objective Indications of Non-Obviousness

Objective indications of non-obviousness include: (1) commercial success, (2) copying, (3) industry praise, (4) skepticism, (5) long-felt but unsolved need, and (6) failure of others. *See*, *e.g.*, *Transocean Offshore Deepwater Drilling, Inc. v. Maersk Drilling U.S., Inc.*, 699 F.3d 1340, 1349–56 (Fed. Cir. 2012). Samsung is not aware of any evidence that would tend to establish any secondary indications of non-obviousness. This lack of evidence further renders the Asserted

Claims obvious. Proving any such secondary considerations is Telcom's burden. *See*, *e.g.*, *ZUP, LLC v. Nach Mfg., Inc.*, 896 F.3d 1365, 1373 (Fed. Cir. 2018) ("[A] patentee bears the burden of production with respect to evidence of secondary considerations of nonobviousness."). Accordingly, Samsung reserves all rights regarding its full contention in this respect until after Telcom completes its final and binding disclosure of any such evidence and contentions. In the meantime, Samsung note the complete lack of any such evidence in the record.

Telcom has disclosed no evidence of, and Samsung knows of no viable evidence to suggest:

The alleged invention's commercial success. No products are known to practice the Asserted Claims. To the extent Telcom asserts that Samsung's products practice the Asserted Patents, Samsung denies that assertion and incorporates its responses to date and any future contentions, expert reports, and testimony. Further, Samsung knows of no nexus between any commercial success and the Asserted Claims. *See, e.g.*, *Windsurfing Int'l Inc. v. AMF*, 782 F.2d 995 (Fed. Cir. 1986) (considerations such as intervening, non-covered technological innovations, popularity of accessories, and advertising expense are all relevant to the nexus determination). If any commercial success is due to any of the concepts discussed in the Asserted Patents, those concepts are also present in the prior art, as described above, and thus do not support any commercial success that is relevant to the question of obviousness. *See Tokai Corp. v. Easton Enters, Inc.*, 632 F.3d 1358, 1369–70 (Fed. Cir. 2011) ("If commercial success is due to an element in the prior art, no nexus exists."); *In re Huai-Hung Kao*, 639 F.3d 1057, 1068 (Fed. Cir. 2011) ("Where the offered secondary consideration actually results from something other than what is both claimed and novel in the claim, there is no nexus to the merits of the claimed invention."); *Ormco Corp. v. Align Tech., Inc.*, 463 F.3d 1299, 1312 (Fed. Cir. 2006) ("[I]f the feature that creates the commercial success was known in the prior art, the success is not pertinent.").

Nor has Telcom presented evidence of commercial success via a licensing program.

Long felt but unresolved needs. Telcom has presented no evidence of any long felt and unresolved need. To the contrary, multiple solutions to the alleged problems pre-dated the Asserted Claims.

Industry praise. There is also no evidence of industry praise for the alleged invention of the Asserted Claims. To the extent any praise is related to any functionality that allegedly practices the Asserted Claims, that praise is not due to any novel features of the Asserted Patents, but instead only to features present in the prior art, which is not a sufficient nexus to be relevant to the question of industry praise for purposes of obviousness. *See Muniauction, Inc. v. Thomson Corp.*, 532 F.3d 1318, 1328 (Fed. Cir. 2008). Praise of Samsung's mobile phones and features is not praise of the Asserted Patents.

Unexpected results. No evidence of any such unexpected results is known. As discussed above, the concepts contained in the Asserted Claims were already combined in the same manner as in those claims. These prior art systems, as described in the above-referenced exhibits, disclosed the same combination of elements, and the same result of that combination, that is recited in the claims. Thus, there were no unexpected results that arose from combining the well-known elements in the Asserted Claims.

The failure of others. No evidence of any such failure is known, and no such failure is associated with a problem that was first solved by the Asserted Claims.

Skepticism by experts. No experts or person of skill expressed skepticism about implementing the alleged inventions.

Teaching away by others. No evidence of any such teaching is known.

Recognition of a problem. As discussed above, the industry recognized the problem and had already discussed multiple approaches that implemented the Asserted Claims to solve that problem.

Copying of the alleged invention by competitors. No evidence of any such copying is known. *See Amazon.com, Inc. v. Barnesandnoble.com, Inc.*, 239 F.3d 1343, 1366 (Fed. Cir. 2001) (allegedly copied feature must be an embodiment of the patented claims).

VII. INVALIDITY UNDER 35 U.S.C. § 112

Pursuant to the Order Governing Proceedings, Samsung identifies below grounds of invalidity under 35 U.S.C. § 112.

A. Legal Background Regarding The Indefiniteness, Enablement, And Written Description Requirements

Section 112, ¶ 2 includes a definiteness requirement: "[T]he specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention." 35 U.S.C. § 112, ¶ 2. "[A] patent is invalid for indefiniteness if its claims, read in light of the patent's specification and prosecution history, fail to inform, with reasonable certainty, those skilled in the art about the scope of the invention." *Nautilus, Inc. v. Biosig Instruments, Inc.*, 134 S. Ct. 2120, 2124 (2014).

The definiteness requirement requires that the claim set forth what the applicant regards as the invention, and do so with sufficient particularity and definiteness. *Allen Eng'g Corp. v. Bartell Indus.*, 299 F.3d 1336, 1348 (Fed. Cir. 2002). Where it would be apparent to one of skill in the art, based on the patent specification, that the "invention" set forth in a claim is not what the patent applicant regarded as the invention, the claim is invalid. *Id.*

35 U.S.C. § 112 further includes an enablement requirement: "The specification shall contain a written description . . . of the manner and process of making and using [the invention] in

such full, clear, concise and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same." 35 U.S.C. § 112, ¶ 1. To satisfy the enablement requirement, the disclosure "must teach those skilled in the art how to make and use the full scope of the claimed invention without 'undue experimentation.'" *Genentech, Inc. v. Novo Nordisk A/S*, 108 F.3d 1361, 1366 (Fed. Cir. 1997); *MagSil Corp. v. Hitachi Glob. Storage Techs., Inc.*, 687 F.3d 1377, 1381 (Fed. Cir. 2012); *Sitrick v. Dreamworks, LLC*, 516 F.3d 993, 999 (Fed. Cir. 2008). If a specification teaches away from a substantial portion of the claim or does not enable the full scope of the claim, there is no enablement. *AK Steel Corp. v. Sollac*, 344 F.3d 1234 (Fed. Cir. 2003); *see also MagSil Corp.*, 687 F.3d at 1383-84 (Fed. Cir. 2012).

35 U.S.C. § 112 further includes a written description requirement: "The specification shall contain a written description of the invention . . . ." 35 U.S.C. § 112, ¶ 1. "To satisfy the written description requirement, a patent applicant must convey with reasonable clarity to those skilled in the art that, as of the filing date sought, he or she was in possession of the invention." *ICU Medical Inc. v. Alaris Medical Systems, Inc.*, 558 F.3d 1368, 1377 (Fed. Cir. 2009) (internal quotation marks and citations omitted); *see also Synthes USA, LLC v. Spinal Kinetics, Inc.*, 734 F.3d 1332, 1340 (Fed. Cir. 2013). "The test [for written description support] requires an objective inquiry into the four corners of the specification from the perspective of a person of ordinary skill in the art. Based on that inquiry, the specification must describe an invention understandable to that skilled artisan and show that the inventor actually invented the invention claimed." *Ariad Pharmaceuticals, Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010) (en banc).

The specification must describe the claimed invention in sufficient detail so that a POSITA can recognize what is claimed. "The appearance of mere indistinct words in a specification or a

claim, even an original claim, does not necessarily satisfy that requirement." *University of Rochester v. G.D. Searle & Co.*, 358 F.3d 916, 923 (Fed. Cir. 2004) (internal quotation marks and citations omitted).

B. Invalidity Grounds Under 35 U.S.C. § 112

Based on Telcom's Infringement Contentions, and subject to the reservations set out above, Samsung identifies grounds upon which it contends that the Asserted Claims are invalid for failure to meet the requirements of 35 U.S.C. § 112 ¶¶ 1, 2 and/or 4. Although its investigation continues, Samsung believes that the Asserted Claims identified below are invalid for failure to comply with 35 U.S.C. § 112 for at least the following reasons: (1) the common specification of the Asserted Patents lacks a written description of the alleged inventions of the Asserted Claims in full, clear, concise, and exact terms as required by 35 U.S.C. § 112 ¶ 1; and/or (2) the common specification of the Asserted Patents does not enable the Asserted Claims as required by 35 U.S.C. § 112 ¶ 1; (3) one or more of the Asserted Claims fail to specify the scope of the claimed inventions with reasonable particularity as required under 35 U.S.C. § 112 ¶ 2. Samsung specifically reserves the right to amend and/or supplement these Invalidity Contentions based on a failure to comply with the requirements of 35 U.S.C. § 112, including, for example, based on supplementation or amendments to Telcom's deficient Infringement Contentions.

The Asserted Claims fail to meet the written description requirement because the alleged inventions claimed therein are not sufficiently described in the common specification of the Asserted Patents. Specifically, the Asserted Claims fail to meet the written description requirement for at least the terms identified below because, based on those terms, the common specification of the Asserted Patents does not adequately convey to those skilled in the art that the inventors had possession of the claimed subject matter as of the filing date. The Asserted Claims additionally fail to meet the enablement requirement because the common specification of the Asserted Patents

does not describe the manner and process of making and using the alleged inventions in the Asserted Claims to enable a person of skill in the art to make and use the full scope of the alleged invention without undue experimentation. Specifically, the Asserted Claims fail to meet the enablement requirement for at least the terms identified below because the common specification of the Asserted Patents does not describe the manner and process of making and using the alleged invention in the Asserted Claims. Based on Samsung's present understanding of the Asserted Claims and Telcom's apparent interpretation of these claims as reflected in its Infringement Contentions, the Asserted Claims may fail to satisfy the requirements of § 112, ¶ 2 because the precise scope of at least the phrases listed below (or terms contained therein) cannot be determined with reasonable certainty by a POSITA when reading the claims in light of the specification and prosecution history.

The Asserted Claims fail the requirements of 35 U.S.C. § 112 in view of at least the following claim terms and phrases:

Asserted Claims[1]	Claim Term	Invalidity Based on 35 U.S.C. § 112
'411 Patent		
All claims	"refraining from communicating"	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"refraining from communicating ... even though the proximity criterion is detected as being satisfied"	Lack of Written Description; Lack of Enablement; Indefinite
'708 Patent		
All claims	"short range link"	Lack of Written Description; Lack of Enablement; Indefinite

[1] Includes unlisted claims that depend from listed claims.

Asserted Claims[1]	Claim Term	Invalidity Based on 35 U.S.C. § 112
All claims	"refraining from communicating"	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"wherein the communicating between the smartphone and the entity using the first air interface … is performed concurrently with the communicating between the smartphone and the base station using the second air interface…"	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"wherein the smartphone receives the communications service from the base station via the second air interface but does not receive the communications service from the entity via the first air interface"	Lack of Written Description; Lack of Enablement; Indefinite
Claim 4 and Claim 14	"selectively sending, by the smartphone, second information to a second device and receiving, by the smartphone, third information from the second device responsive to the proximity criterion having been satisfied between the smartphone and the entity,"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 5, 15, 16, 17, 18, and 19	"over a point-to-point short-range link between the smartphone and the entity using a time division duplex protocol"	Lack of Written Description; Lack of Enablement; Indefinite
Claim 6	"enabling a function by the smartphone"	Lack of Written Description; Lack of Enablement; Indefinite
Claim 10	"wherein the method further comprises sending the information to a second device"	Lack of Written Description; Lack of Enablement; Indefinite

Asserted Claims[1]	Claim Term	Invalidity Based on 35 U.S.C. § 112
'199 Patent		
All claims	"wireless short-range communications link"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 4, 7, 14, 17	"short-range signal"	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"wirelessly providing by the smartphone, using the first air interface, information to the entity and wirelessly receiving by the smartphone, using the first air interface, information from the entity independently of, and absent involving the entity in, receiving by the smartphone the communications service from the wireless network using the second air interface	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"wirelessly receiving by the smartphone, using the second air interface, the communications service from the wireless network absent involving the entity, absent providing by the smartphone information to the entity, and absent receiving by the smartphone information from the entity"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 2, 11	"wherein said wirelessly providing by the smartphone … is performed over a first time interval; wherein said wirelessly receiving by the smartphone … is performed over a second time interval; and wherein the first and second time intervals are non-overlapping with one another"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 7 and 17, Claims 8 and 18.	"performing a transaction"	Lack of Written Description; Lack of Enablement

Asserted Claims[1]	Claim Term	Invalidity Based on 35 U.S.C. § 112
	"performing a financial transaction"	
'432 Patent		
All claims	"performing a plurality of financial transactions"	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"first data relating to a plurality of financial transactions to be conducted"	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"second data relating to a plurality of financial transactions to be conducted"	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"performing a first transaction"	Lack of Written Description; Lack of Enablement
All claims	"short-range communications link"	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"short-range signal"	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"independent of performing said first transaction, receiving by the smartphone a communications service from a wireless network, using a second air interface that differs from the first air interface"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 5, 14	"performing a second transaction of the plurality of financial transactions"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 5, 14	"second entity"	Lack of Written Description; Lack of Enablement
Claim 6, 15	"a first device"	Indefinite

Asserted Claims[1]	Claim Term	Invalidity Based on 35 U.S.C. § 112
Claim 8, 17	"causing data to be transmitted selectively to a plurality of predetermined devices and further causing data to be received selectively from said plurality of predetermined devices"	Indefinite
'756 Patent		
Claims 1-10	"responsive to the value that is determined by the device for the parameter that is sensed satisfying a threshold criterion, enabling by the device a number of functions of the device and disabling by the device a function of the device"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 1-10	"disabling … a function of the device"	Lack of Written Description; Lack of Enablement; Indefinite
Claim 4	"conducting by the device the financial transaction by paying for a product"	Lack of Written Description; Lack of Enablement
Claims 11-13	"responsive to the value that is sensed satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 11-18	"disabling a function of the wireless device"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 14-18	"responsive to the value satisfying the threshold criterion, enabling a number of functions of the wireless device and disabling a function of the wireless device;"	Lack of Written Description; Lack of Enablement; Indefinite

Asserted Claims[1]	Claim Term	Invalidity Based on 35 U.S.C. § 112
Claims 5, 13, 16	"enabling at the second device a function for conducting the financial transaction."	Lack of Written Description; Lack of Enablement; Indefinite
Claims 11, 14	"using the function for conducting the financial transaction and conducting the financial transaction by paying for a product"	Lack of Written Description; Lack of Enablement
Claim 17	"a short-range wireless link with the entity"	Lack of Written Description; Lack of Enablement; Indefinite
Claim 18	"a wireless link that comprises a distance that is greater than a distance associated with the proximity condition"	Lack of Written Description; Lack of Enablement; Indefinite
'743 Patent		
All claims	"master-slave relationship"	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"selectively establishing a master-slave relationship"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 2, 9	"maintain enabled a first function of the smartphone while maintaining disabled a second function of the smartphone"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 2, 9	"maintaining enabled said first function while maintaining disabled said second function responsive to deciding that said value of the parameter continues to satisfy the criterion"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 2, 9	"disabling said first function and enabling said second function responsive to deciding that the value	Lack of Written Description; Lack of Enablement; Indefinite

Asserted Claims[1]	Claim Term	Invalidity Based on 35 U.S.C. § 112
	of the parameter no longer satisfies the criterion"	
Claims 3, 10	"using the capability to conduct the financial transaction that has been established at the smartphone and conducting the financial transaction by paying for a product"	Lack of Written Description; Lack of Enablement
Claims 3, 10	"short-range signal"	Lack of Written Description; Lack of Enablement
Claims 7, 14	"enabling a first function of the smartphone while disabling a second function of the smartphone responsive to sensing the parameter and responsive to determining that the parameter sensed satisfies the criterion"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 6, 13	"short-range link"	Lack of Written Description; Lack of Enablement; Indefinite
'172 Patent		
All claims	"short-range signal"	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"paying for a product by selectively sending information to at least one device"	Lack of Written Description; Lack of Enablement
All claims	"wherein said performing the second step of said two-step process comprises sensing …, determining …. and then, …, paying for a product by selectively sending information to at least one device;"	Lack of Written Description; Lack of Enablement; Indefinite

Asserted Claims[1]	Claim Term	Invalidity Based on 35 U.S.C. § 112
Claims 2, 10	"enabling a first function of the smartphone while disabling a second function of the smartphone responsive to the at least one parameter having been sensed"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 2, 10	"communications capability of the first function"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 2, 10	"master-slave relationship"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 3, 11	"whether or not to maintain enabled said first function while maintaining disabled said second function"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 3, 11	"disabling said first function and enabling said second function responsive to deciding that the value of the at least one parameter no longer satisfies the criterion"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 5, 13	"causing data to be transmitted selectively to at least one device and further causing data to be received selectively from at least one device"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 5, 13	"performing a financial transaction"	Indefinite
'793 Patent		
All claims	"using the function that has been established to conduct the financial transaction and conducting the financial transaction by paying for a product"	Lack of Written Description; Lack of Enablement
All claims	"short-range signal"	Lack of Written Description; Lack of Enablement; Indefinite

Asserted Claims[1]	Claim Term	Invalidity Based on 35 U.S.C. § 112
Claims 4, 9, 11	"short-range link"	Lack of Written Description; Lack of Enablement; Indefinite
Claim 7	"short-range wireless link"	Lack of Written Description; Lack of Enablement; Indefinite
All claims	"paying for the product by selectively sending information to at least one device"	Lack of Written Description; Lack of Enablement
All claims	"wherein said paying for a product further comprises deducting/withdrawing an amount of money from an account"	Lack of Written Description; Lack of Enablement
All claims	"wherein said paying for a product comprises sensing … , determining … and then, … , paying for the product by selectively sending information to at least one device"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 2, 6	"enabling at least one first function comprises enabling the at least one first function and disabling a second function"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 2, 6	"disabling"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 2, 6	"whether or not to maintain enabled said at least one first function while maintaining disabled said second function"	Lack of Written Description; Lack of Enablement; Indefinite
Claims 2, 6	"maintaining enabled said at least one first function while maintaining disabled said second function responsive to deciding that the physiological parameter sensed satisfies the criterion"	Lack of Written Description; Lack of Enablement; Indefinite

Asserted Claims[1]	Claim Term	Invalidity Based on 35 U.S.C. § 112
Claims 2, 6	"disabling said at least one first function and enabling said second function responsive to deciding that the physiological parameter sensed no longer satisfies the criterion"	Lack of Written Description; Lack of Enablement; Indefinite

Samsung reserves the right to modify, amend, or supplement its contentions relating to 35 U.S.C. § 112 as the case progresses, including in view of any claim construction orders entered by the Court in this matter.

VIII. INVALIDITY UNDER 35 U.S.C. § 101

Pursuant to Judge Gilstrap's Standing Order, Exhibits 411-C, 708-C, 199-C, 432-C, 756-C, 743-C, 172-C, and 793-C provide charts identifying (1) each exception to eligibility (e.g., abstract idea, law of nature, and natural phenomenon) to which each Asserted Claim of the Asserted Patents is directed and the factual and legal basis therefor; (2) whether one or more of the Asserted Claims of the Asserted Patents are representative of any other claims; (3) a description of the industry, at the relevant time, in which the Asserted Claims of the Asserted Patents are alleged to be well understood, routine, and conventional, and the factual and legal basis therefor; (4) a description of how each element of the Asserted Claims of the Asserted Patents, both individually and in combination with the other elements of that claim, was well understood, routine, conventional, in the relevant industry at the relevant time, and the legal and factual basis therefor; and (5) any other factual or legal basis for how the Asserted Claims of the Asserted Patents are otherwise ineligible for patent protection.

Samsung further incorporated by reference the Section 101 briefing on the asserted patents submitted by Apply in *Telcom Ventures LLC v. Apple, Inc.*, Case No. 1:24-cv-23837-JEM (S.D. Fl.) (*see* Dkt. Nos. 28, 34).

These Ineligibility Contentions, like the rest of these Invalidity Contentions and the exhibits hereto, are based on the facts and law currently available to Samsung, and Samsung reserves the right to update these contentions in light of additional cases and guidance as they become available, the Court's claim construction order, or positions Telcom takes on infringement.

IX. DOCUMENT PRODUCTION ACCOMPANYING INVALIDITY CONTENTIONS

With these Invalidity Contentions and Subject Matter Eligibility Contentions, Samsung produces the documents required under Local Patent Rule 3-4 and the Standing Order Regarding Subject Matter Eligibility Contentions Applicable to All Patent Infringement Cases Assigned to Chief District Judge Rodney Gilstrap, as ordered on 25 July, 2019.

Dated: August 27, 2025

/s/ Kevin Hardy

Sean Pak (*pro hac vice*)
seanpak@quinnemanuel.com
Iman Lordgooei (admitted in E.D. Tex.)
imanlordgooei@quinnemanuel.com
QUINN EMANUEL URQUHART & SULLIVAN, LLP
50 California Street, 22nd Floor
San Francisco, California 94111
Telephone: (415) 875-6600
Facsimile: (415) 875-6700

Kevin Hardy
D.C. Bar No. 473941 (admitted in E.D. Tex.)
kevinhardy@quinnemanuel.com
QUINN EMANUEL URQUHART & SULLIVAN, LLP
1300 I Street, N.W., Suite 900
Washington, DC 20005
Telephone: (202) 538-8000
Facsimile: (202) 538-8100
Attorney for Defendants
Samsung Electronics America, Inc. and
Samsung Electronics Co., Ltd.

CERTIFICATE OF SERVICE

Pursuant to the Federal Rules of Civil Procedure and Local Rule CV-5, I hereby certify that, on August 27, 2025, all counsel of record who have appeared in this case are being served with a copy of the foregoing via email.

Dated: August 27, 2025

/s/ Benjamin M. Kleinman
Benjamin M. Kleinman