EXHIBIT A

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS

PROXENSE, LLC,

Plaintiffs,

v.

SAMSUNG ELECTRONICS, CO., LTD. and
SAMSUNG ELECTRONICS AMERICA, INC,

Defendants.

Civil Action No. 6:21-cv-00210-ADA

INFRINGEMENT CONTENTIONS FOR US PATENT NO. 8,352,730

U.S. Patent Number 8,352,730 – Preliminary Infringement Contentions[1]

Assignee:	Proxense, LLC
Title:	Biometric personal data key (PDK) authentication
Filing Date:	2005-12-20
Publication Date:	2013-01-08
Inventor:	Giobbi, John J.

'730 Patent Claim[2]		**Accused Instrumentality And Where Each Claim E**
1	A method for verifying a user during authentication of an integrated device, comprising the steps of[4]:	Samsung Pay preloaded[5] smartphones carry out the cla the doctrine of equivalents, for at least the reasons set f
	persistently storing biometric data of the user and a plurality of codes and other data values comprising a device ID code uniquely identifying the integrated device and a secret decryption value in a tamper proof format written to a storage element on the integrated device that is unable to be subsequently altered;	<u>persistently storing biometric data of the user … in a ta to a storage element on the integrated device that is una altered</u> Utilizing the Android operating system, Samsu persistently store biometric data of the user in a

[1] The Preliminary Infringement Contentions (PICS) provided herein are based on information obtained to date and may not be exhaustive. Plain infringement is ongoing. Plaintiff reserves the right to supplement and/or amend these PICS to identify additional instrumentalities and to furthe each claim is found in each accused instrumentality, including on the basis of discovery obtained from Defendants, and from third-parties durin pursuant to ¶2 of the Order Governing Proceedings – Patent Cases under Hon. Alan D. Albright.

[2] All PICS set forth herein for any independent patent claims are hereby incorporated by reference into the PICS alleged for any dependent pate independent claims, as if fully set forth therein.

[3] The Accused Instrumentalities and associated exhibits discussed and/or cited for any claim herein are representative in all material respects of identified for that claim (e.g., a specified Samsung Galaxy phone may be used as a representative example in these charts since the other accuse differences in their hardware and/or software configuration, the cited references are believed to be illustrative of all such accused devices).

[4] Plaintiff's inclusion of any claim preamble in this claim chart should not be interpreted as an admission that the preamble is limiting. Plaintiff position that the claim preambles are limiting or not limiting on a claim-by-claim basis.

[5] For the avoidance of doubt, "preloaded" includes devices that ship with Samsung Pay pre-installed or upon which Samsung Pay is otherwise i

‘730 Patent Claim[2]	Accused Instrumentality And Where Each Claim E
	to a storage element on the integrated device th subsequently altered. Starting with the Galaxy S6 and S6 Edge, Sams preloaded with Samsung Pay. Samsung Newsroom, *Samsung’s Unpacked Ev Mobile World Congress* (2015), http://news.sar unpacked-event-to-set-the-pace-for-mobile-wo S6 and S6 edge will come with Samsung Pay, a universally accepted mobile payment system th credit cards, debit cards and NFC.”); Cho Jin-y *Samsung Pay in Its All Smartphone Starting fro* http://www.businesskorea.co.kr/news/articleVi .html?idxno=16767 (“An official from Samsun December 14, ‘We have decided to pre-install S Electronic’s smartphone to be released from ne Samsung’s devices persistently store user biom in connection with Samsung Pay. “To add an e user’s] Samsung Pay account, [users] can turn Fingerprint or Iris Verification.” Set up Samsun https://www.samsung.com/us/support/answer/A storage of user biometric data on Samsung dev fingerprint or iris template of the user, to verify fingerprint or iris against. Samsung Pay preloaded smartphones utilize the biometric data, Android’s implementation guid “raw fingerprint data or derivatives (for exampl never be accessible from outside the sensor dri execution environment) and “fingerprint acquis recognition must occur inside the TEE”. Andro Fingerprint HIDL, https://source.android.com/secruity/authenticat Requiring acquisition and recognition to occur

‘730 Patent Claim[2]	Accused Instrumentality And Where Each Claim E
	following the implementation guidelines, finge TEE. Android’s TEE, called Trusty, “uses AR virtualize the main processor and create a secu environment” isolated from the rest of the syste Project: Trusty TEE, https://source.android.con Accordingly, fingerprint data, which never leav leaves the Trustzone housing, Trusty. Keeping Trustzone, Android phones, including Samsung Pay, can persistently store biometric data in a ta Samsung Pay admittedly adheres to Android’s Specifically, Samsung Pay utilizes Samsung Kn Samsung Knox and tokenization add extra laye Pay, https://www.samsung.com/us/samsung-pa utilizing Knox, “the authentication software do biometric measurements of any user.” Knox Pl Version 1.3.1 (2020), page 41. “The measurem that can’t be used to reproduce the original bion accessed and decoded within the specific part o access to the biometric hardware.” *Id*. Ensurin within a specific part of the Trustzone can acce Samsung Knox keeps biometric information wi to Android’s implementation guidelines. On Android devices (like the Samsung devices Pay), access to the biometric hardware is contro “Android uses Fingerprint Hardware Interface l to connect to a vendor-specific library and fing example, a fingerprint sensor).” Android Open HIDL, https://source.android.com/secruity/auth Only permitting access to biometric informatio to biometric hardware, Samsung Pay preloaded must limit access to fingerprint biometric data t Fingerprint HIDL. The methods enabled by th permit altering biometric data. *Id*. (providing a

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**