Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 24 November 2023

Case Number: T 0220/21 - 3.5.01

Application Number: 16705884.1

Publication Number: 3254248

IPC: G06Q20/40

Language of the proceedings: EN

Title of invention:
BIOMETRIC MEASURES PROFILING ANALYTICS

Applicant:
Fair Isaac Corporation

Headword:
Biometric profiling/FAIR ISAAC

Relevant legal provisions:
EPC Art. 52(2), 56

Keyword:
Inventive step - (no - obvious implementation of non-technical requirements)

Decisions cited:
T 1901/08

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 0220/21 - 3.5.01

D E C I S I O N
of Technical Board of Appeal 3.5.01
of 24 November 2023

Appellant: (Applicant)	Fair Isaac Corporation 181 Metro Drive Suite 700 San Jose, CA 95110 (US)
Representative:	Müller-Boré & Partner Patentanwälte PartG mbB Friedenheimer Brücke 21 80639 München (DE)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 9 November 2020 refusing European patent application No. 16705884.1 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chairman	N. Glaser
Members:	L. Falò
	L. Basterreix

Summary of Facts and Submissions

I. This is an appeal against the examining division's decision to refuse European patent application No. 16 705 884.1.

II. The application was refused on the grounds of lack of inventive step of all requests in view of a known client-server computer system.

III. In the statement setting out the grounds of appeal, the appellant requested that the decision of the examining division be set aside and that a patent be granted on the basis of the refused main request or of one of the refused first to third auxiliary requests, all re-filed therewith.

IV. In the communication pursuant to Article 15(1) of the Rules of Procedure of the Boards of Appeal, the Board informed the appellant that it tended to agree with the contested decision and was therefore minded to dismiss the appeal.

V. In a letter of reply, the appellant announced that it would not attend the oral proceedings, withdrew the request for oral proceedings and requested "a decision according to the state of the file".

VI. Oral proceedings were held as a videoconference on 24 November 2023. As announced, nobody appeared for the appellant. The Chairperson announced the decision at the end of the oral proceedings.

VII. Claim 1 of the main request reads:

A method comprising:

collecting (102), by a capturing device connected with at least one data processor, biometric data associated with a consumer;

determining (104), by at least one data processor, one or more biometric variables associated with the consumer, each of the one or more biometric variables representing a measurable aspect of the biometric data;

calibrating, by at least one data processor, the biometric data to a common scale, the calibrating comprising the at least one data processor executing real-time recursive quantile estimation to recast the one or more biometric variables into dimensionless values digitally expressed as a real-time estimate of quantiles of a biometric profile variable distribution, the calibrating by the at least one data processor enabling the biometric profile variable distribution to change over time and within different segments of consumers and devices associated with the consumers;

generating (106), by at least one data processor and based on at least one of the one or more biometric variables, at least one biometric profile variable associated with the consumer, the at least one biometric profile variable representing a degree of normality or abnormality of the collected and calibrated biometric data as compared to a biometric history of the consumer according to the common scale;

comparing, by the at least one data processor, the at least one biometric profile variable to at least one global biometric profile variable, the at least one

global biometric profile variable representing a distribution of the at least one of the one or more biometric variables determined from a population of other capturing devices associated with one or more users different from the consumer;

calculating, by the at least one data processor and based on the comparing, a scaled value indicating whether a value of the at least one biometric profile variable comprises an outlier value, the outlier value comprising a value above a threshold quantile of the distribution of the at least one of the one or more biometric variables determined from the population of other capturing devices associated with the one or more users different from the consumer;

generating (108), by at least one data processor, a behavioral score for the consumer based on the collected and calibrated biometric data, the scaled value, and at least one biometric profile variable, the behavioral score representing a degree of normality or abnormality of an biometric event associated with the history of biometric data; and

authenticating, by the at least one data processor and based on the behavioral score, a transaction associated with the consumer.

VIII. Claim 1 of the first auxiliary request adds to the end of the "generating (106)" step "*the degree of normality or abnormality of the collected and calibrated biometric data indicating typical biometric match levels over time;*"

IX. Claim 1 of the second auxiliary request further adds to the end of claim 1:

"wherein the biometric data includes one or more of the following usage behaviors of a mobile device:
B-party called, the B-party indicating destination numbers,
B-party texts,
B-party MMS,
URL visited,
apps running,
data downloaded,
data requested,
location with latitude and longitude,
wifi networks connected,
gyro position of a mobile phone as the mobile device,
step motion on a mobile phone as the mobile device,
power on or power off,
jail broken,
sleep mode,
system setting changes,
keystroke monitoring and/or swipes."

X. Claim 1 of the third auxiliary request further adds to the end of the "collecting (102)" step "*the capturing device being a mobile device associated with the consumer*", and replaces, after the "authenticating" step, the expression "*a mobile device*" with "*the mobile device*".

XI. The appellant's arguments can be summarised as follows:

The goal of the invention is not to prevent fraud, as argued by the examining division, but to authenticate a transaction and provide better terminal security. These are inherently technical goals, as confirmed in decision T 1901/08, and are further achieved by technical means, which include capturing biometric

data, determining a measurable aspect thereof, calibrating the data and determine a degree of normality or abnormality. The definition of the data to be captured has a technical character because it implies technical considerations concerning the functioning of a mobile phone.

Reasons for the Decision

1. The invention concerns using biometric data to detect fraud, for example in the context of financial transactions (see paragraphs [006], [007], [0023]) or to analyse and classify customer behaviour ([008]). In the context of the invention, the expression "biometric data" may indicate physiological data, such as retinal scan, fingerprint, facial recognition, DNS (known as "high-friction biometric data", [0020] to [0022]), as well as behavioral data reflecting the user's interaction with a mobile device, such as numbers called, location, URL visited ("low-friction biometric data", [006], [007]). The expression "friction" indicates how much customers or users are encumbered by a process, or to what extent they have to pay attention to the process, see [004].

Prior art methods of analysing biometric data by performing a matching of pre-stored biometric markers are said to be error-prone and/or give a high rate of false positives. This is because the quality of the data collected varies with the measurement device used, the user's skills in taking the measurement, and environmental conditions.

According to the description, the invention increases

the accuracy of the biometric profiling and reduces the number of false positives ([007]).

To achieve this, biometric data collected by a capture device ([0020], [0021]) are calibrated to a common scale, processed to extract at least one biometric variable and compared with a consumer history to generate a biometric profile variable, which represents a degree of normality or abnormality of the collected data ([009]). The biometric profile variable can be further compared to a global biometric profile variable, representing a distribution within a certain population, to determine a "scaled value" indicating the presence of outlier values ([0037] to [0047]). The biometric profile variable and the scaled value are used to calculate a "behavioral score" for the consumer and, based thereupon, decide whether to authenticate a transaction associated with the consumer ([009], [0023], [0037]).

2. The examining division refused claim 1 of all requests in view of a known client-server system. Documents D1, US 2014/337225 and D2, US 2007/233614 were cited as examples thereof.

3. The appellant argued that the method of claim 1 was not directed to preventing fraud, as argued by the examining division, but to the authentication of a transaction, and that the overall aim of the invention was to improve authentication in a computer system or to provide better terminal security. These were inherently technical goals, as could be derived from decision T 1901/08.

Moreover, these goals were achieved by technical means, which included capturing specific types of biometric

data, determining a measurable aspect thereof, calibrating the data so as to facilitate comparison of current data with past data, and determining a degree of normality or abnormality. All the claimed features required a technical understanding of the machine on which they were implemented and of the functioning of a mobile phone. A human being would not calculate a behavioural score, but only carry out a visual comparison of the captured data with reference values.

Third auxiliary request - inventive step

4. The Board finds it expedient to start with the assessment of the most specific third auxiliary request.

5. The Board agrees with the assessment of technicality carried out by the division and, in particular, with the identification of the only technical aspects of the invention, which are a known client-server computer system wherein the client is a mobile device associated with the user. These technical means implement an abstract, non-technical scheme for the authentication of a transaction based on a consumer's behaviour.

6. As argued by the appellant, the invention can be considered to be directed to the authentication of transactions. However, in the Board's view this is not a technical goal, but a business-oriented or administrative one. It is therefore *per se* insufficient to lend technicality to the claimed subject-matter. Indeed, according to the application the transactions may be financial transactions, while the "authentication" merely indicates the execution of a generic action associated with the transaction, based

on an assessment of the associated risk (see for example the description, paragraph [0023]).

7. Also the idea of assessing the transaction risk, based on detected statistical anomalies in the users' behaviour, compared with their past behaviour and with that of a reference population is considered non-technical, as its formulation does not require any kind of technical consideration or expertise, but only reflects heuristic assumptions as to what may constitute a "suspicious" behavior.

8. It is self-evident that only measurable quantities can be detected by technical means. Hence, the feature of determining one or more variables representing a measurable aspect of the biometric data, even when considered technical, is implicit in any computer-based implementation, or at least an obvious consequence thereof, and cannot establish an inventive step.

9. The appellant argued that the specific choice of the type of data to be captured, as listed at the end of the claim, implied a technical understanding of the functioning of a mobile device.

However, the Board observes that at least the use of the "location with latitude and longitude" or "jail broken" criteria does not require any such understanding. The remaining items on the list are only claimed as possible alternatives and concern well known, commonplace types of interaction between a user and a mobile device, particularly a smart phone. Hence, they represent obvious possibilities for the skilled person.

10. The steps concerning the calibration of data, the generation of a biometric profile variable, the calculation of the "scaled value" and the generation of the "behavioural score" are mathematical methods, which are inherently non-technical (Article 52(2)(a) EPC). The calculated behavioural score does not have a technical significance and, moreover, is used for a non-technical purpose, namely to authenticate a transaction associated with a consumer.

Contrary to the appellant's arguments, the Board is of the opinion that the use of numerical values does not imply, *per se*, technical considerations concerning the functioning of a computer and, more generally, is not sufficient to confer technicality to the claimed subject-matter. If this were the case, any mathematical method would be technical. Moreover, the Board does not see any plausible reason which would prevent a human being from carrying out a quantitative analysis of the behavioural data.

11. In decision T 1901/08, the Board found that the detection of a particular type of fraud relied on a technical understanding of a terminal and of its components and, in particular, on the recognition that the jamming of a card reader in combination with another condition signal of a component of the terminal was indicative of a tamper attempt (see reasons, point 3.1.3 of the decision).

The present case is different. As discussed above, the criteria used for authenticating transactions are not based on a technical understanding of the functioning of the implementing devices, i.e. the capturing device and the data processors. In particular, and contrary to the appellant's arguments, the Board cannot identify

any feature in the claim which credibly improves the security of these devices.

12. Accordingly, the Board concludes that the subject-matter of claim 1 is an obvious implementation, on notoriously known technical means, of a non-technical scheme for authenticating transactions. Therefore, the claim lacks an inventive step (Article 56 EPC).

Main, first and second auxiliary requests - inventive step

13. Claim 1 of the higher ranking requests is more general than claim 1 of the third auxiliary request. Hence, the same objections as to a lack of inventive step apply, mutatis mutandis.

Conclusion

14. As none of the appellant's requests is allowable, the appeal must be dismissed.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chairman:

T. Buschek N. Glaser

Decision electronically authenticated