Viktoria Veres

info.vveres@gmail.com

GIVING `FACE` TO NON-FACE-TO-FACE CLIENT IDENTIFICATION

Absztrakt

A gyorsan fejlődő modern ügyfél-azonosítási és átvilágítási technológiák széleskörűen integrálható azonosítási es autentikációs megoldásai egyre inkább helyettesíthetővé teszik a klasszikus, közvetlen módszereket. A cégek hamarosan képesek lesznek kényelmesen, költség- és időhatékonyan, a jól ismert ügyviteli, pénzügyi és pénzmosással összefüggő kockázatok minimalizálása mellett is, biztonsággal azonosítani akár a világ másik részén lévő leendő ügyfeleiket. Ebben a cikkben a szerző a tradicionális, teljes körű ügyfél-azonosítás kiváltására, egy kizárólag online ügyfélkapcsolat létesítése során alkalmas lehetséges azonosítási megoldást mutat be, annak előnyeivel és korlátaival.

Abstract

Traditional Face-to-face Client Identification methods are more and more replaceable by rapidly developing modern technology giving wide range of options to unify identification, authentication and validation methods into one real time system. Soon businesses will be able to identify and authenticate prospective Clients located on the other side of the globe in a cost and time efficient, convenient way while minimizing well known operational, credit and money laundering risks. This article presents a possible scenario with its advantages and limitations to switch to real time online distance verification from the traditional face-to-face client identification.

Keywords: Client Identification, Biometrics, Face recognition, eCommerz

Giving a Face to Non-face-to-face Client Identification

Growing number of online companies fall under special domestic and international regulations, standards to keep up with the challenges of Client authentication and identification on the daily basis. The internal risk management incorporate operational, credit, legal, reputation and other risks that are determined by a wide range of company specific elements, including company culture, compliance costs, loss tolerance in both quantitative (e.g. money lost) and qualitative areas (e.g. reputation)[1] require flexible procedures to be mitigated. Nevertheless, risk management considerations will ascertain the Company`s goal and level to comply with Client identification, validation and transaction authentication, processing standards.

Though the identification of Clients to establish a business relationship is a long required condition for specific industries and fields, new technologies, like biometrics[2], have only been adapted where capturing data is through specially developed and installed devices, such as fingerprint or iris readers placed in the premises of the business and for limited use such as to access accounts or services. These new technologies including face recognition is getting more are more popular for marketing and VIP service purposes in bank branches [3] and voice recognition is used more often used instead of security questions in phone banking[4]. Unfortunately, are still not used for the initial identification, authentication and validation of Clients[5]. The goal of this article is to draft an alternative solution for a common problem of online companies that fall under the above mentioned client identification, client due

[1] KPMG: Understanding and articulating risk appetite 2008
http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/Risk-appetite-O-200806.pdf
Last viewed: 15.04.2013

[2] Biometris can be described by physiological and behavioral characteristics of a human body.
Security In E-Banking Via Card Less Biometric Atms in International Journal of Advanced Technology & Engineering Research (IJATER) Volume 2, Issue 4, July 2012 ISSN No: 2250-3536 p.10, also available online http://www.ijater.com/Files/9a989a3d-b5ec-4f5d-a837-fbbb9649d1e6_IJATER_05_02.pdf Last viewed 15.04.2013

[3] Techshino: VIP Customers Face Recognition Precise Positioning System
http://en.techshino.com/solution/detail.html?id=10 last viewed 15.04. 2013

[4] Derek du Preez: Barclays adopts voice biometrics for customer identification Computerworld UK 2013
http://www.computerworlduk.com/news/applications/3446244/barclays-adopts-voice-biometrics-for-customer-identification/ last viewed 15.04.2013

[5] Identification is to capture Clients data (e.g checking someones ID for his name, date of birth, picture, signature), authentication is to check the given data set exists (e.g the address or the name in the ID exists in other databases) and vaildation/verification means to make sure the existing data is valid for the person whose identity is checked, the individual is who they claim to be (e.g. the person is not abusing someone elses data).

diligence, age verification regulatory requirements or would like enhanced internal risk and fraud management. Are state of the art Know-Your-Client and Due Diligence tools and methods closer to us than we think?

The face-to-face identification requirement

An online service provider company with limited physical geographical presence and wide range of international Clients is obligated to perform face-to-face personal and address identification and/or age verification from the beginning of the business relationship mostly through checking the original or official third party attested personal documents of the Client without or with very limited options for Risk Based Approach[6] Such requirement is for example that ``Banks should establish a systematic procedure for identifying new customers and should not establish a banking relationship until the identity of a new customer is satisfactorily verified.``[7]

While globalization and technology is encouraging people to engage in wordwide online activities, services, purchase goods, keep their money in eMoney accounts, regulators seemingly all agree and prefer face-to-face identification even if the `online life` and business model conditions do not make it as favorable and convenient as in the classic branch banking industry. ``AML/CFT legislation requires obliged entities to know their customers – as well as certain other persons who are not always their customers (e.g. beneficial owners) – and to assess their associated ML/TF risks. For that purpose, obliged entities need to collect, process and record personal data, and sometimes to share such data with public authorities (such as FIUs) or with private entities within the same group. These requirements have implications for such persons with respect to their rights regarding respect of private life and protection of personal data while having an overall security impact (general interest).``[8]

The most common Client identification is still through something a person has, an ID card, a passport, a driver`s license, a social security number, a utility bill. In a bank branch Clients

[6] This article does not examine the identification requirements of Clients other than private persons, therefore companies, beneficial owners, PEPs etc are not referred to when using the word Client or Clients.

[7] Basel Committee on Banking Supervision: Customer due diligence for banks 01.11.2011 http://www.bis.org/publ/bcbs85.pdf p.6 Last viewed 15.04.2013

[8] European Commission: Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing and Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds 2013 http://ec.europa.eu/internalmarket/company/docs/financial-crime/130205impact-assessment_en.pdf p.52-53 Last viewed 15.04.2013

can access their established bank account by presenting and ID to get immediate access and control of their funds. The clerk will ask some additional simple questions and/or answers to confirm (postal address or the name of my mother) based on something the Clients know. The identification is therefore through something the person has and something the Client knows[9], both are easy to get, alter and reproduce at a basic level, as the Clerk has no real time tool to authenticate and verify the format and details of the presented identification document. First time Client identification at the account setup phase may be therefore the most crucial to be made extensively.

The challenges

Most of the regulators obligate companies for face-to-face identification of their Client where the business environment does not support it. Contradictions and limited options give companies continuous difficulties to understand and comply with regulations and standards. Some of these are collected hereby:

- no physical option for in-house face-to-face identification– e.g. the company does not have branch in the country or area of the Client
- face-to-face identification through own personnel that may not able to spot faked documents – e.g more and more high quality fake documents are produced that cannot be validated without computerized methods
- too expensive registered/official third party identification for the Client – e.g. through notary, accountant, lawyer, embassy, post office (Germany PostIdent is up to 7 euro, accountant 50 euro, lawyer 80 euro per full set of identity documents)
- forbidden 3rd party identity confirmation – e.g. regulated banks are not willing to confirm the data of their identified Clients to others, like eMoney companies, financial services, high value good sellers, auction houses, due to strict privacy laws and the lack of appropriate domestic and international information sharing framework
- no national and international databases to use for details authentication during the identification process, and if they exist the single source identification without face-to-face meeting is not always enough to meet regulatory requirements (e.g. Schufa in Germany)

[9] Especially if the ID is issued abroad with which the Clerk is not up to date or experienced

- too low amount is involved to make economic sense for any kind of financial abuse, therefore the face-to-face identification requirement may be irrelevant
- multiple identification obligation through the same methods even if the flow of funds were through regulated banking system (Client is already verified the traditional way)
- an obligation to store copies identity documents or the opposite, it is forbidden to request and store any sensitive data related documents in online operation
- no common, easily accessible, trustworthy national and international rules and standards to cover clients from different countries

Besides the difficulties there are several positive examples on jurisdictions that recognize the nature and needs of the online industry and allow alternative identification methods for non-face to face clients[10]. Canada and the United Kingdom supports companies in different industry fields to use data aggregators, credit files and deposit account confirmations[11] to crosscheck the details obtained at the account opening phase of their business relationship with the Client.[12]

In India, VISA launched a new program with several participating banks to use biometric technology to avoid misuse of bank accounts by false identification of Clients, with the coordination of the government: ``Both the account and the associated biometric data are securely hosted by the new national identity system, which is run by the Unique Identification Authority of India (UIDAI)``.[13]

Also the new draft of the EU 4th money laundering directive is giving more space for the member states to redefine the low risk clients that does not need more due diligence[14] (by far low risk were almost only face-to-face Clients), expresses the importance of Risk Based

[10] Clients who do not present themselves and their identification document in one of the company`s premises

[11] A minimum of two combinations of identification details must match. Deposit account confirmation may be a security number sent within a minor transaction to the Clients bank account that the Client needs to confirm back to the Company.

[12] FINTRAC, CANAFE: New PCMLTFA Obligations Money Services Businesses 2008 http://www.fintrac-canafe.gc.ca/publications/presentations/pre-ped/pdf/2008-02-00-msb-esm-eng.pdf Last viewed: 15.04.2013

[13] VISA: Visa Launches New Payment Service in India – Links Indian Unique Identification with Visa Accounts http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1766726&highlight=

[14] CFE Professional Affairs Committee: Opinion Statement of the CFE on the proposal for a 4th Anti Money Laundering DirectiveCOM (2013) 45 04.2003 http://www.cfe-eutax.org/sites/default/files/CFE%20Opinion%20Statement%20on%20the%20proposal%20for%20a%204th%20EU%20Anti%20Money%20Laundering%20Directive.pdf p.3 last viewed 15.04. 2013

Approach and most importantly confirms that ``electronic fund transfers below €1,000 are not subject to identity verification`, [15]

Interesting recent statement of the CFE Professional Affairs Committee submitted to the European Institutions even goes further and expresses that face-to-face client identification will not bring better money laundering reporting results, even saying the lack of verification would not change the amount of suspicious transactions reported by tax advisors. ``Identification and verification of clients cause the bulk of the administrative burden for the obliged entities but in the tax advisers´ practice, it is not through these processes that indications for money laundering are identified but through the insight in the past transactions of the clients. Therefore, based on our experience, it is fair to say that if there was only a reporting obligation and no verification obligation except in high risk situations, probably the amount and quality of the reports would remain the same.``[16]

These examples show that the use of alternative methods for Client identification is getting into the spotlight of decision makers.

Moving to complex and high level identification – giving face to a non-face-to-face identification

As we saw traditional face-to-face identification and personal data authentication in a global company environment is hard to achieve due to the legal requirements are not aligned with the new tech options for modern, efficient, cheap and convenient Client identification.

According to the Basel Committee statements regarding Customer Due Diligence for banks: ``The best documents for verifying the identity of customers are those most difficult to obtain illicitly and to counterfeit...``[17] But what if not documents are the single best for identification and we can use something that is the hardest to obtain by another person?

[15] European Commission: Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing and Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds 2013 http://ec.europa.eu/internal_market/company/docs/financial-crime/130205_impact-assessment_en.pdf p.83 Last viewed 15.04.2013

[16] CFE Professional Affairs Committee: Opinion Statement of the CFE on the proposal for a 4th Anti Money Laundering Directive COM (2013) 15 04.2013 http://www.cfe-eutax.org/sites/default/files/CFE%20Opinion%20Statement%20on%20the%20proposal%20for%20a%204th%20EU%20Anti%20Money%20Laundering%20Directive.pdf p.3 Last viewed 15.04. 2013

[17] Basel Committee on Banking Supervision: Customer due diligence for banks 11.2001 http://www.bis.org/publ/bcbs85.pdf p.6 Last viewed 01.03.2013

We can identify users or Clients by something *they know, they have, and they are.*[18] Practice shows that the security level of identification is increasing once the factor `something you are` is involved. `Something you are` can be best and only authenticated by biometric solutions, as these include physical or behavioral elements that someone possesses and do not or not frequently change. [19] Therefore something `you have` and `something you know` can be accessed, stolen, reproduced, misunderstood more easily as any unique feature of a specific person.

The below figure shows the most performed combination for identification and authentication, as we move upwards to more complex identification it becomes more and more used only for internal personnel authentication and less applied for Clients.

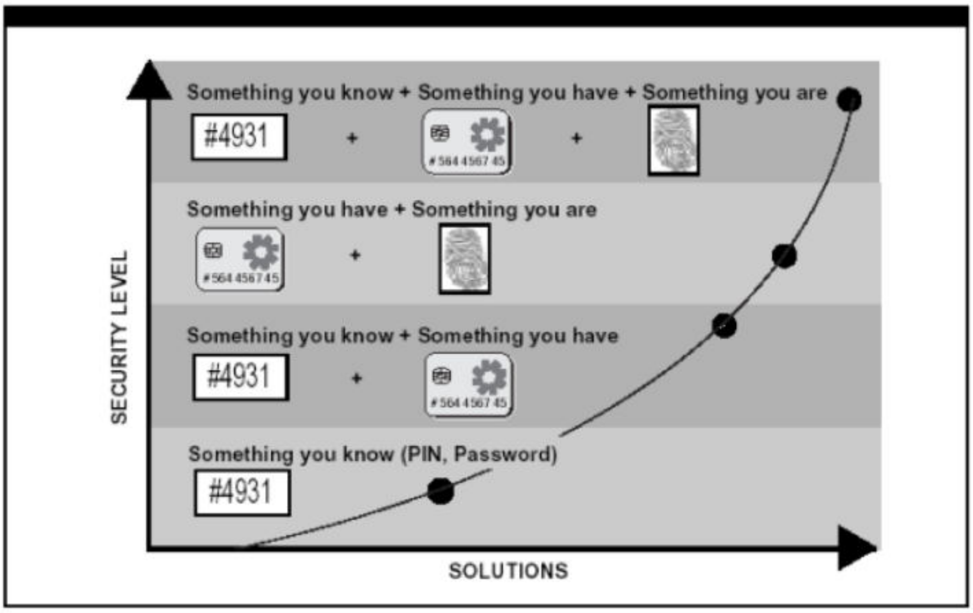

Something you know + Something you have + Something you are
#4931
+
#564 4567 45
+
Something you have + Something you are
#564 4567 45
+
Something you know + Something you have
#4931
+
#564 4567 45
Something you know (PIN, Password)
#4931
SECURITY LEVEL
SOLUTIONS

Figure 1: Security level and identification/authentication methods used[20]

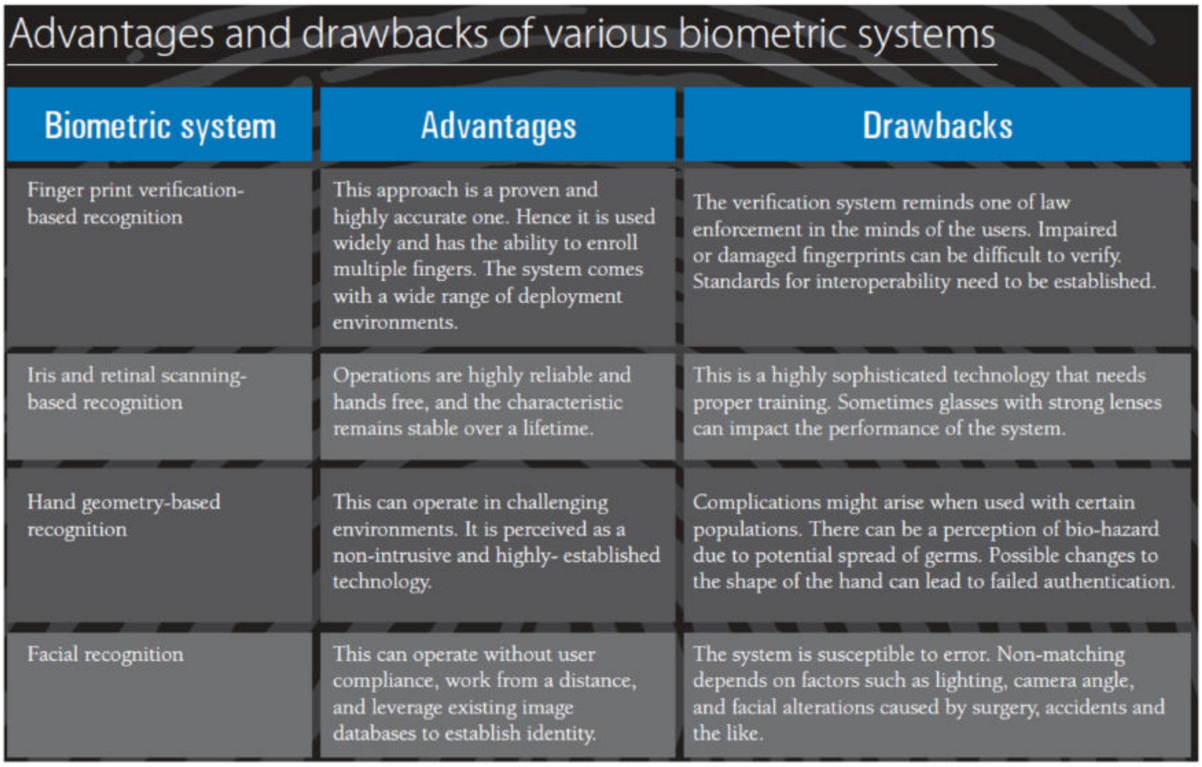
Striving for more security, big organizations and companies such as banks, auction houses and other widely used service providers all over the world started to add more and more biometric authentication to their everyday Client relationships, not only to ATM accesses, branch authentications, telephone banking but also internet banking and online purchases.

[18] Abhishek Kumar Sinha: Financial Transactions get personalized and secure with Biometrics http://www.infosys.com/FINsights/Documents/pdf/issue10/financial-transactions.pdf p.5 15.04.2013

[19] Smart Card Alliance: Smart Cards and Biometrics in Privacy Sensitive Secure Personal Identification Systems 05.2002 http://www.smartcardalliance.org/resources/lib/Biometrics_and_Smart_Cards_Report.pdf p.11 Last viewed: 03.09.2012

[20] Same as above, p.18

According to an open source internet research, 121 banks in the world use biometrics, mostly fingerprint and hand vein reading methods. Asian and third world countries are leading the biometric authentication and identification share in banking relationships, but often only for ATM use and branch banking access.[21] The below table shows the main reasons why hand-geometry based recognition and fingerprint verification became so popular among them.



Advantages and drawbacks of various biometric systems

Biometric system	Advantages	Drawbacks
Finger print verification-based recognition	This approach is a proven and highly accurate one. Hence it is used widely and has the ability to enroll multiple fingers. The system comes with a wide range of deployment environments.	The verification system reminds one of law enforcement in the minds of the users. Impaired or damaged fingerprints can be difficult to verify. Standards for interoperability need to be established.
Iris and retinal scanning-based recognition	Operations are highly reliable and hands free, and the characteristic remains stable over a lifetime.	This is a highly sophisticated technology that needs proper training. Sometimes glasses with strong lenses can impact the performance of the system.
Hand geometry-based recognition	This can operate in challenging environments. It is perceived as a non-intrusive and highly- established technology.	Complications might arise when used with certain populations. There can be a perception of bio-hazard due to potential spread of germs. Possible changes to the shape of the hand can lead to failed authentication.
Facial recognition	This can operate without user compliance, work from a distance, and leverage existing image databases to establish identity.	The system is susceptible to error. Non-matching depends on factors such as lighting, camera angle, and facial alterations caused by surgery, accidents and the like.

Figure 2: Advantages and drawbacks on various biometric methods[22]

Additionally we may update the tool with online identity `something that is public/online of you` or so called `unregulated RealIDs`, which would give a further layer of authentication.[23] As the research published by Heinz College & CyLab and the Carnegie Mellon University University states: ``….a world where anyone may run face recognition on anyone else, online and offline``[24]

[21] Seyyede Samine Hosseini, Dr. Shahriar Mohammadi: Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System in Journal of Basic and Applied Scientific Research http://www.textroad.com/pdf/JBASR/J.%20Basic.%20Appl.%20Sci.%20Res.,%202%289%299152-9160,%202012.pdf also under ISSN ISSN 2090-4304 p.9155-9159 Last viewed 15.04.2013

[22] Abhishek Kumar Sinha p.4 Last viewed 15.04. 2013

[23] Alessandro Acquisti, Ralph Gross, Fred Stutzman: Faces of Facebook: Privacy in the Age of Augmented Reality http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf

[24] Same as above

Merging online and offline data (captured traditionally and/or through biometrics) of a person may lead us stepping away from face-to-face identification and entering a more complex system of proving identity even without the active participation of the Client. Online face recognition researches not only focus on finding out who the person is by connecting the face to publicly available information (e.g. Facebook, LinkedIn as shown on the below in Figure 3) but also on how we can predict personal information from images. [25]

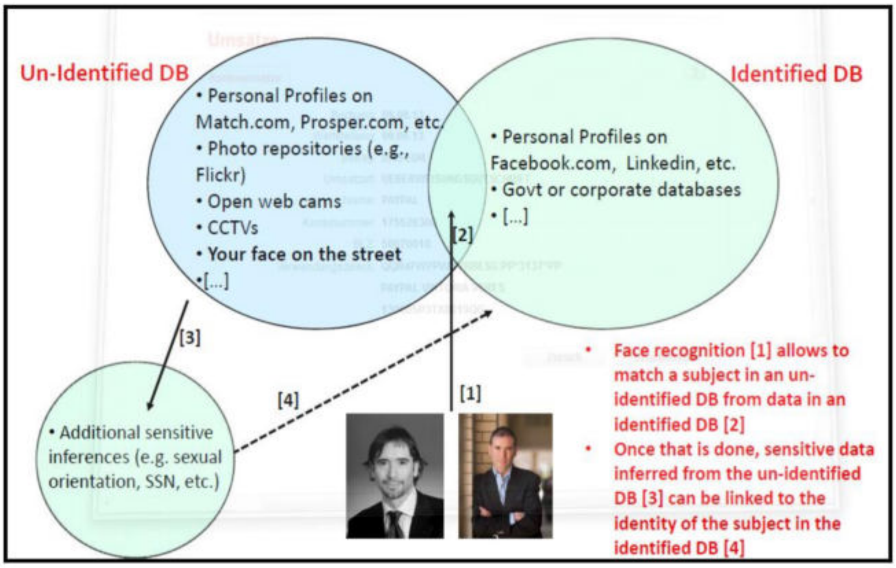

Un-Identified DB
• Personal Profiles on Match.com, Prosper.com, etc.
• Photo repositories (e.g., Flickr)
• Open web cams
• CCTVs
• Your face on the street
•[...]
Identified DB
• Personal Profiles on Facebook.com, Linkedin, etc.
• Govt or corporate databases
• [...]
[2]
[3]
[4]
[1]
• Additional sensitive inferences (e.g. sexual orientation, SSN, etc.)
• Face recognition [1] allows to match a subject in an un-identified DB from data in an identified DB [2]
• Once that is done, sensitive data inferred from the un-identified DB [3] can be linked to the identity of the subject in the identified DB [4]

Figure 3: Matching captured faces to un-identified and identified databases[26]

The main question is if using additional layers of identification is increasing the accurateness and secureness of Client identification, authentication and verification. If biometrics supported identification is one of the most accurate method, in combination with additional layers, can it be confidently used instead of the traditional face-to-face methods?

Face-to-face identification is mostly presenting our ID and utility bill to a clerk, shop personnel or sending it by fax/email to the seller or service provider. If the clerk has no option to double check our details in national or cross national databases - for example a Polish ID when opening a German bank account – and no option to authenticate the card structure and

[25] Same as above
[26] Same as above

quality itself (pixeling, holograms, format and text comprehensiveness, etc.), the clerk has to rely on what he sees on the ID card and the Client who is standing in front of him. Several researches showed the limitations of human mind recognizing faces and two dimensional codes.[27] The Clerk will copy his documents and the bank will keep it as hard copy for certain amount of years stated in regulations. (Upon opening the bank account in some countries where credit check systems exists the bank will report the details of the Client to the national credit rating system with the data captured by the clerk. If the identity document was fake, the bank will forward the fake data to the central system, from where all the rest of the companies may verify the identity of the Client or take a decision on engaging in business relationship or not.)

Doing a same procedure through real time video connection with the Client using face recognition programs and we can receive personal documents through an online system that evaluates and scores the comprehensiveness of the scans, while the video compares the camera picture of the Client with his presented ID card and to other publicly available information[28] - may lead to:

- the real time computerized document validation giving a higher level certainty that the presented identification documents were not faked, altered or modified
- the ability to check if the captured biometric data of the face matches to the ID picture (or any other records in the database)[29] – less human mistakes, less chance for collusion between Clerk and Client
- checking the person`s identity in publicly available systems, such as social networks[30] to obtain more data for evaluation
- age identification connected to real time face evaluation, may assist with old ID pictures, in some cases the software can evaluate the ageing since the ID picture was taken[31]

[27] Theo Pavlidis: Computers versus Humans 23.12.2012 http://www.theopavlidis.com/comphumans/comphuman.htm Last viewed 15.04.2013

[28] The accuracy of the clerks` decisiveness through the multi layered online system on fake or real identity would be with high probability the same as by a face-to-face client

[29] Atul Gupta, Vikas Dewangan, V.V Ravi Prasad: Facial recognition in Infosys http://www.infosys.com/microsoft/resource-center/Documents/facial-recognition-technology.pdf p. 3 Last viewed 15.04.2013

[30] Alessandro Acquisti, Ralph Gross, Fred Stutzman: Faces of Facebook: Privacy in the Age of Augmented Reality http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf

[31] Atul Gupta, Vikas Dewangan, V.V Ravi Prasad p.9 Last viewed 15.04.2013

- Immediate blacklist screening using the captured data and biometric data, reducing fraud and money laundering risk[32]
- voice recognition can be a reference for future other service usage[33] (phone banking, ATM)
- personalized experience – VIP banking, targeted marketing based on biometric logins or appearance[34], convenience of engaging into business relationship and fulfilling identification requirements from home
- full audit trail of the identification process, more data captured, more can be forwarded and used in case of official financial fraud and money laundering investigations
- reduced branching time, less physical paper storage need, reduced coverall costs[35]
- higher data accuracy, higher Client satisfaction[36], no queuing

It is not recommended to fully switch off the human element of the identification verification process, therefore for first time distance Client boarding a video call is essential. Advantage of the system, that while the Client and Clerk is having a conversation of the services or goods, the system captures the data and evaluates the new client automatically. The human element may also help to increase the Client`s confidence in biometrics and to avoid the feeling of invading their privacy.

The concerns

There are some concerns and limits regarding integrating to everyday purchase and service use (with emphasis on becoming a new Client through state of art methods) a multi-layer identification and authentication involving biometrics, especially in case of the face recognition Current limits of using face recognition through the Clients home computer:

Clients not willing to enroll through their system, they may feel to invading to capture their face sitting at home. It is not recommended to fully switch off the human element of the identification verification process, therefore for first time distance Client boarding a video call

[32] Abhishek Kumar Sinha p.10 Last viewed: 15.04.2013
[33] Abhishek Kumar Sinha p.10 Last viewed: 15.04.2013
[34] Atul Gupta, Vikas Dewangan, V.V Ravi Prasad p.8 Last viewed 15.04.2013
[35] Seyyede Samine Hosseini, Dr. Shahriar Mohammadi: Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System in Journal of Basic and Applied Scientific Research http://www.textroad.com/pdf/JBASR/J.%20Basic.%20Appl.%20Sci.%20Res.,%202%289%299152-9160,%202012.pdf also under ISSN ISSN 2090-4304 p. 9152
[36] Abhishek Kumar Sinha p.10 Last viewed 15.04.2013

is essential. Advantage of the system, that while the Client and Clerk is having a conversation of the services or goods, the system captures the data and evaluates the new client automatically. The human element may also help to increase the Client`s confidence in biometrics and to avoid the feeling of invading their privacy.

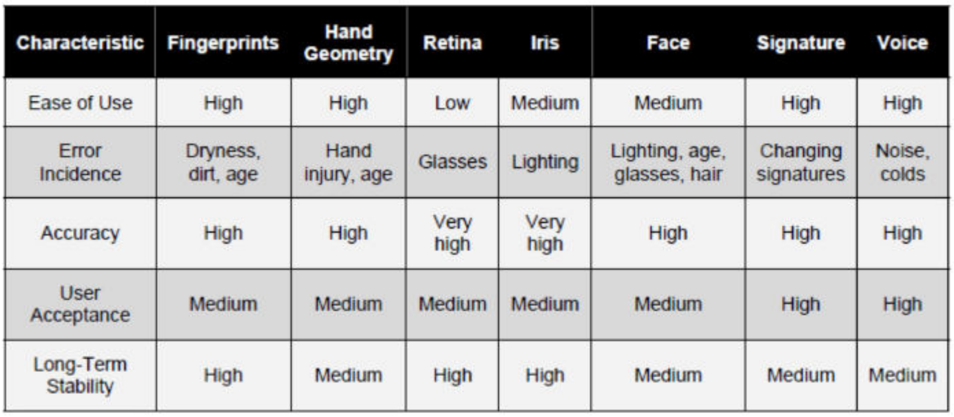
Average PC cameras are not able to capture enough accurate data for face analysis and people tend to have mobile devices that have less capacity for high quality camera features. Rapid industry developments shows that this limitation eliminated, the latest phones have the right technology and features to be used for distance Client identification purposes. Smartphones already use face and voice recognition for unlocking the device, latest smartphone developments try to increase the quality of these features, therefore the accuracy and acceptance level of these recognition methods may boom in the coming months.[37] The problem still remains in less developed areas where the access to these high-end devices is limited.

Challenges of data acquiring, detecting, aligning, extracting due to object failures.[38] Face recognition is susceptible to error and many factors influence the accuracy (see Figure 2). These factors can be controlled as the Clerk can instruct the Client what to do (e.g. switch on the light or take off the glasses) in order overcome the failures and mismatches.

Accuracy of the data processing is not under the acceptable false positive/correct negative level (using the combination may reach this level). Looking at the table below (Figure 4) we can see that the face and voice identification may be the same reliable accurate as fingerprints and hand geometry. At the moment there are not enough researches that can show us what would be the accuracy and acceptable failure rate of an identification system where only one element is the face recognition.

[37] Soycincau: Samsung develops own Face Unlock which requires you to blink 29.03.2012 http://www.soyacincau.com/2012/03/29/samsung-develops-own-face-unlock-which-requires-you-to-blink/ Last viewed: 15.04.2013

[38] Atul Gupta, Vikas Dewangan, V.V Ravi Prasad: Facial recognition in Infosis http://www.infosys.com/microsoft/resource-center/Documents/facial-recognition-technology.pdf p.10 Last viewed 15.04.2013



Characteristic	Fingerprints	Hand Geometry	Retina	Iris	Face	Signature	Voice
Ease of Use	High	High	Low	Medium	Medium	High	High
Error Incidence	Dryness, dirt, age	Hand injury, age	Glasses	Lighting	Lighting, age, glasses, hair	Changing signatures	Noise, colds
Accuracy	High	High	Very high	Very high	High	High	High
User Acceptance	Medium	Medium	Medium	Medium	Medium	High	High
Long-Term Stability	High	Medium	High	High	Medium	Medium	Medium

Figure 4: Comparing of biometric technologies[39]

Privacy laws and slow adaptation of regulators. Privacy laws and anti-money laundering laws are still too strict and different in various countries, therefore sellers and service providers on international market may find difficulties to introduce distance identification, authentication and validation methods to their global operation.

Technology is too costly and security requirements may be difficult to meet. In connection to the above statement, due to the relatively high implementation and maintenance costs, if not all geographical areas can be covered and Clients the system may not be economic.

As a summary we can say that the main challenges of the multi-layer client identification and authentication include possible refusal of the society to link online purchase/service use activity to their integrated online and offline identity, high costs of having multiple systems analyzing unstructured client data and aggregating it to one unified system and the lack of regulatory framework and standards for using complex real time layering system.

What the future holds

Traditional Face-to-face Client Identification methods are more and more challenged by the rapidly developing modern technology that not only may capture and validate more data but gives wide range of options to unify identification, authentication and validation methods into one real time system even without significant human interaction. Soon businesses will be able to identify and authenticate Clients located on the other side of the

[39] Smart Card Alliance p.10 Last viewed: 03.09.2012

globe in a cost and time efficient, convenient way while minimizing well known operational, credit and money laundering risks. In order to be able to confidently switch to distance identification technological development to lower false identification ratio is not enough, there needs to be a wide acceptance of the society and regulatory decision makers. The main problem of the use of biometrics, especially face recognition is that unlike using PIN numbers, they use the human body and behavior elements that people consider to invasive to collect by online companies. At the moment biometrics are only used as an additional layer to the document based identification in eCommerz, distance Client identification using face recognition integrated with other authentication and validation methods are not yet spread.

People tend to trust biometric solutions if these are implemented by banks, the financial industry therefore online banks are good incubators for the new methods. There is an implementation limitation due to a high costs of system though that slower the process. Online companies tend to be more interested in methods that can help them to reduce losses from fraud and keep compliance efforts low, compared to traditional companies where being high level compliant with account opening regulations for anti-money laundering is a top priority (they may not be motivated implementing a complex system of distance account opening because they have a well-built infrastructure for face-to-face identification). On the other hand, online companies that are not compliant at the moment with the face-to-face identification laws due to their business model and other limitations discussed in this article and therefore may lose significant markets, may lead the way to prove distance identification can be more accurate and efficient with the right technology, methods and policies. Introducing to the Client Identification process a PC or mobile phone camera based face recognition can be a good first step and `test case` from them.

Early adaptation therefore may be dependent on the supporting regulations that recognize the additional opportunities in a complex, biometrics, document authentication, public information and behavior based client identification and fraud screening systems. If regulators will give more relaxed environment and options to online companies to use the advanced options of the online world for Client Identification and Due Diligence the field will flourish rapidly leading to significant advantages and growing opportunities for all the involved industries from technology providers through risk analyzers, end user businesses, state anti-money laundering units and of course the Clients themselves.

Bibliography

Abhishek Kumar Sinha: Financial Transactions get personalized and secure with Biometrics http://www.infosys.com/FINsights/Documents/pdf/issue10/financial-transactions.pdf p.5 15.04. 2013

Alessandro Acquisti, Ralph Gross, Fred Stutzman: Faces of Facebook: Privacy in the Age of Augmented Reality http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/acquisti-faces-BLACKHAT-draft.pdf

Atul Gupta, Vikas Dewangan, V.V Ravi Prasad: Facial recognition in Infosys http://www.infosys.com/microsoft/resource-center/Documents/facial-recognition-technology.pdf p. 3 Last viewed 15.04.2013

Basel Committee on Banking Supervision: Customer due diligence for banks 11.2001 http://www.bis.org/publ/bcbs85.pdf p.6 Last viewed 01.03.2013

CFE Professional Affairs Committee: Opinion Statement of the CFE on the proposal for a 4th Anti Money Laundering DirectiveCOM (2013) 45 04.2003 http://www.cfe-eutax.org/sites/default/files/CFE%20Opinion%20Statement%20on%20the%20proposal%20for%20a%204th%20EU%20Anti%20Money%20Laundering%20Directive.pdf p.3 last viewed 15.04.2013

Derek du Preez: Barclays adopts voice biometrics for customer identification Computerworld UK http://www.computerworlduk.com/news/applications/3446244/barclays-adopts-voice-biometrics-for-customer-identification/ Last viewed 15.04.2013

European Commission: Impact Assessment accompanying the Proposal for a Directive of the European Parliament and of the Council on the prevention of the use of the financial system for the purpose of money laundering, including terrorist financing and Proposal for a Regulation of the European Parliament and of the Council on information accompanying transfers of funds 2013 http://ec.europa.eu/internal_market/company/docs/financial-crime/130205_impact-assessment_en.pdf p.52-53 Last viewed 15.04.2013

FINTRAC, CANAFE: New PCMLTFA Obligations Money Services Businesses 2008 http://www.fintrac-canafe.gc.ca/publications/presentations/pre-ped/pdf/2008-02-00-msb-esm-eng.pdf Last viewed: 15.04.2013

KPMG: Understanding and articulating risk appetite 2008 http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Documents/Risk-appetite-O-200806.pdf Last viewed: 15.04.2013

Security In E-Banking Via Card Less Biometric Atms in International Journal of Advanced Technology & Engineering Research (IJATER) Volume 2, Issue 4, July 2012 ISSN No: 2250-3536 p.10, also available online http://www.ijater.com/Files/9a989a3d-b5ec-4f5d-a837-fbbb9649d1e6_IJATER_05_02.pdf Last viewed 15.04. 2013

Seyyede Samine Hosseini, Dr. Shahriar Mohammadi: Review Banking on Biometric in the World's Banks and Introducing a Biometric Model for Iran's Banking System in Journal of Basic and Applied Scientific Research http://www.textroad.com/pdf/JBASR/J.%20Basic.%20Appl.%20Sci.%20Res.,%202%289%299152-9160,%202012.pdf also under ISSN ISSN 2090-4304 p.9155-9159 Last viewed 15.04. 2013

Smart Card Alliance:Smart Cards and Biometrics in Privacy Sensitive Secure Personal Identification Systems 05.2002 http://www.smartcardalliance.org/resources/lib/Biometrics_and_Smart_Cards_Report.pdf p.11 Last viewed: 03.09.2012

Soycincau: Samsung develops own Face Unlock which requires you to blink 29.03.2012 http://www.soyacincau.com/2012/03/29/samsung-develops-own-face-unlock-which-requires-you-to-blink/ Last viewed: 15. 04. 2013

Techshino: VIP Customers Face Recognition Precise Positioning System http://en.techshino.com/solution/detail.html?id=10 Last viewed 15.04.2013

Theo Pavlidis: Computers versus Humans 23.12.2012 http://www.theopavlidis.com/comphumans/comphuman.htm Last viewed 15.04.2013

VISA: Visa Launches New Payment Service in India – Links Indian Unique Identification with Visa Accounts http://pressreleases.visa.com/phoenix.zhtml?c=215693&p=irol-newsarticlePR&ID=1766726&highlight= Last viewed 15. 04. 2013