Omni-Channel Customer Engagement
Security & Biometrics

White Paper

The role of Biometrics in the new era of digital services.

Improve the security of electronic payments with biometric authentication.

NUANCE

To help you comply with the new regulatory framework applicable to payments in the European Union, Nuance delivers industry-leading biometric solutions designed to help financial services organizations carry out transactions with the highest level of security and a frictionless customer experience.

Payment Services Directive 2

The second Payment Services Directive ("**PSD2**")[1] is part of a global trend in bank regulation emphasizing security, innovation, and market competition. The PSD2 took effect on 13 January 2018, with an initial extension until 14 September 2019, followed by another extension until 31 December 2020. The extension was authorized by the EBA in order to facilitate the compliance of all affected companies. The PSD2 aims to modernize Europe's payment services to the benefit of both consumers and businesses. Thus, it enables businesses to keep pace with a rapidly evolving market, while enhancing consumer protection against fraud and liability accountability across the payment ecosystem.

In the words of Valdis Dombrovskis[2] *"This legislation is another step towards a digital single market in the EU. It will promote the development of innovative online and mobile payments, which will benefit the economy and growth."*

The new European directive not only seeks to reflect technological change, but to promote digital innovation by facilitating the market entry of new types of payment service providers. It also aims to provide greater transparency over transactions, to improve consumer protection and strengthen the security of payments.

PSD2: Key changes

- Creates an equal playing field for payment service providers by enabling new third-party companies to get into the payments ecosystem.
- Includes more transaction types within scope, such as transactions in new geographical regions and currencies (outside the Member States and the Euro).
- Regulates new payment services apart from credit cards and transfers between bank accounts, such as payment initiation and account information.
- Strengthens security requirements, including Strong Customer Authentication (SCA) and new consumer protections.
- Introduces controls related to unauthorized payment fraud cases and liability of the payment service provider. If an unauthorized payment operation is carried out, the payer's payment service provider will be liable for reimbursing the amount of the unauthorized operation immediately.

[1] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market

[2] Vice-President responsible for Financial Stability, Financial Services and Capital Markets Union

What makes PSD2 so different

OPEN BANKING

PSD2 will be a key catalyst for finally making “Open Banking” a reality. The new payment initiation and account information services will provide opportunities for new entrants to disrupt the European payments framework. These changes present both a challenge (due to the risk of disintermediation) and an opportunity (due to existing expertise and infrastructure for financial institutions).

CONSUMER PROTECTION

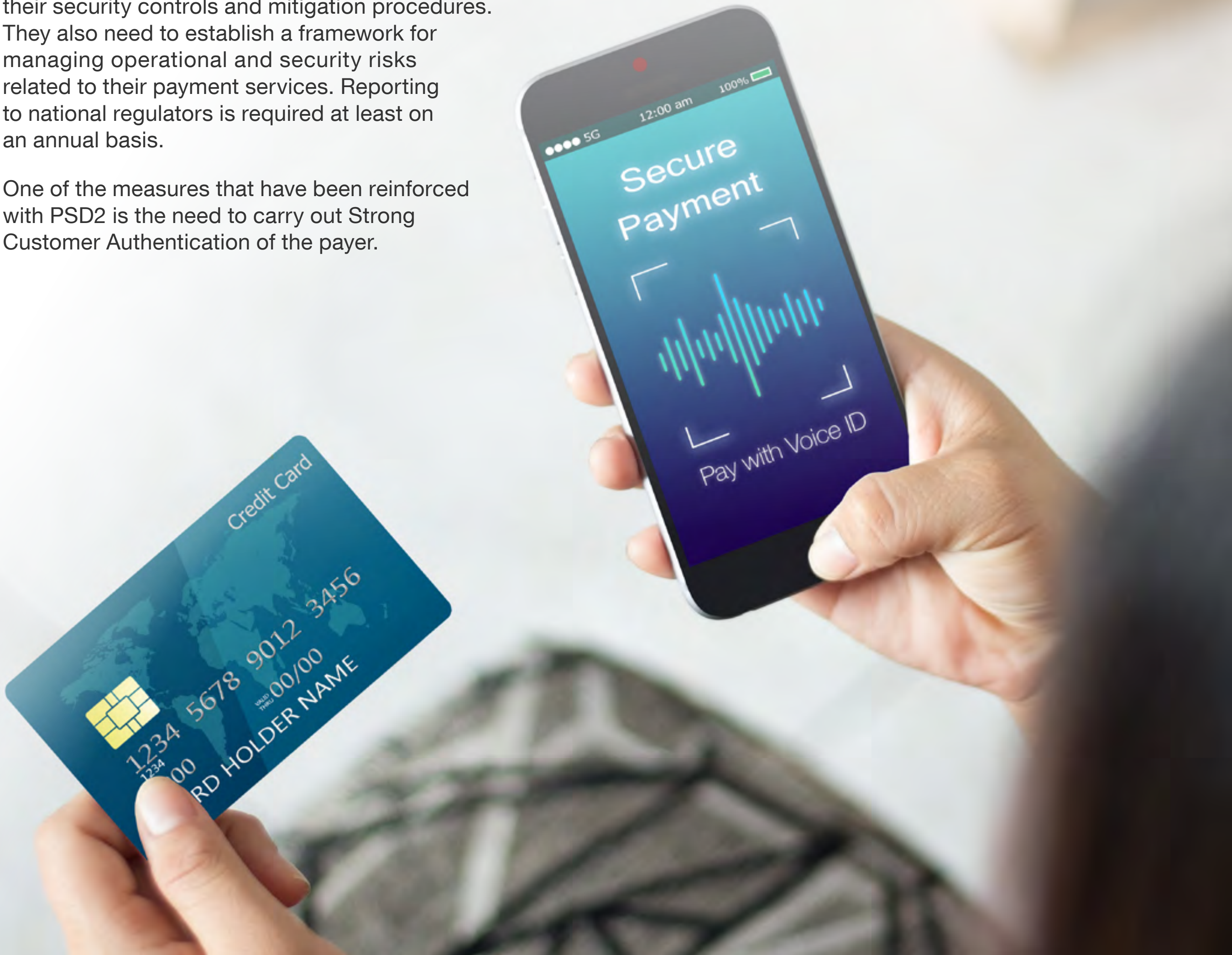
Increased transparency of costs and protection from charges will boost consumer protection. In response to growing cybercrime and online fraud, PSD2 continues the trend towards enhancing the security of payments. The bank or financial services organization would be responsible for unauthorized payments, unless they can demonstrate that the operation was duly authenticated and was not affected by a technical failure.

SECURITY OF PAYMENTS

The security risks relating to electronic payments have increased in recent years, in part due to the increasing technical complexity, the ever-growing volume of electronic payments, and the development of new types of payment services. PSD2 places responsibility for security risks on payment service providers and aims to mitigate them through a clear and harmonized regulatory framework.

Payment services providers must have a security policy document, which includes a detailed risk assessment, a description of their security controls and mitigation procedures. They also need to establish a framework for managing operational and security risks related to their payment services. Reporting to national regulators is required at least on an annual basis.

One of the measures that have been reinforced with PSD2 is the need to carry out Strong Customer Authentication of the payer.



Strong Customer Authentication (SCA)

One of the main pillars of PSD2 is Strong Customer Authentication (SCA), a new European regulatory requirement to make online payments more secure in order to reduce fraud.

To process payments from the effective date of SCA (31 December 2020)[3], at least two factors from the three categories below must be used.

Knowledge	Possession	Inherence
Something that only the user **knows** (PIN, password, etc.)	Something that only the user **possesses** (credit card, RSA token, etc.)	Something that only the user **is** (voice recognition, face recognition, behavioral biometrics ...)

Payment service providers must use Strong Customer Authentication whenever customers access a payment account online and initiate an electronic payment transaction, or carry out “any action, through a remote channel which may imply a risk of payment fraud or other abuses.”

In addition, some remote payment transactions, including payments over the internet and smart phones, must “dynamically link” the transaction to a specific amount and to a specific payee, generating a unique authentication code. As a result of dynamic linking, any change in the amount or the identity of the payee will invalidate the code.

[3] The European Banking Authority (EBA) authorized an extension of the entry into force period. It will not come into effect until 31 December 2020.

Impact of Strong Customer Authentication on financial services

The requirement to apply SCA will affect the payments industry as a whole and, particularly, financial services organizations. The requirement to implement strong customer authentication covering browser-based and mobile payments will drive changes across financial services organizations.

To enable Strong Customer Authentication, most financial services organizations have opted for maintaining the sending of a code or PIN (One Time Password) via SMS. **While the combination of OTP via SMS (a possession element) and a knowledge element, such a password, technically meets the need to have two factors, the underlying assumption is that the customer's possession of the device receiving the OTP is secure. However, the reality is far from that.**

Article 22(4) of the "Regulatory Technical Standards on strong customer authentication and secure communication under PSD2"" states that "Payment service providers shall ensure that the processing and routing of personalised security credentials and of the authentication codes generated in accordance with Chapter 2 take place in secure environments in accordance with strong and widely recognised industry standards."

Increasingly widespread fraud based on account takeovers and SIM replacements (SIM Swapping) reveals a clear lack of security in the environments referred to in the previous article. This presents a strong reason for financial services organizations to discard OTP / SMS for the implementation of enhanced client authentication, as is becoming widespread in the German financial services industry.

Financial services organizations such as Postbank, Raiffeisen Bank, Volksbank and Consorsbank have announced their intention to ban OTP / SMS during 2020, while Deutsche Bank and Commerzbank will act along the same lines, and many others likely to follow suit.

The responsibility of financial services organizations related to SCA

PSD2 represents an essential step towards increased consumer protection in case of loss, theft, misappropriation, and incorrect execution. Payment Service Providers (PSPs) become fully responsible for payments that were not correctly executed. As a consequence they have the obligation to refund the total amount of the unauthorized payment transaction immediately to their clients.

Only when payment services users act fraudulently, or out of gross negligence, are they fully liable.

Therefore, in order to comply with PSD2, it is crucial for financial services organizations to implement a method for strong and secure customer authentication that minimizes to a great extent the risk of identity theft, thereby maximizing client trust and minimizing the costs associated with fraud.

PSD2 compliance has become one of the top priorities for payment service operators given that non-compliance makes them responsible for fraud damages suffered by their clients.

The emerging role of biometrics

In order to implement secure customer authentication, organizations are increasingly looking at biometrics as an optimal authentication approach that can boost both security and customer experience. Combined with a possession or knowledge element, biometrics can help you achieve secure two-factor authentication without the unnecessary friction.

With the prevalence of biometric authentication, such as fingerprint and facial recognition, in many smart phone and tablet devices, users have become accustomed to biometrics as a secure and convenient alternative to passwords.

Organizations looking to leverage biometrics for secure customer authentication need to keep in mind the following considerations:

- **Leveraging native device biometric authentication vs non-native biometric methods:** while leveraging biometric authentication methods that are embedded in everyday mobile devices can simplify implementations, it is important to note that not all native device methods provide a high level of security, accuracy and protection against presentation attacks. Non-native device methods enable organizations to provide more consistent security and experience regardless of the device manufacturer or model. Additionally, depending on the biometrics provider, non-native methods typically provide higher levels of accuracy and anti-spoofing capabilities.
- **Device-side vs server-side biometric processing:** device-side biometric processing ensures that biometric data never leaves the device, so organizations do not need to manage enrollment, processing and matching. However, server-side biometric processing enables the use of the same biometric across multiple channels, such as using a voice print with a mobile banking app and when the customer calls the contact center. Additionally, server-side biometric enrollment provides greater protection against fraud.
- **Choice of biometric modalities:** passive modalities, such as behavioral biometrics, have become more popular as a frictionless, invisible and effective way to provide continuous authentication in web and mobile channels. Additionally, biometric modalities that leverage sensors that are available across a wide range of devices (such as facial, voice and fingerprint biometrics) are also preferred for their familiarity and convenience.
- **Applicable channels:** while PSD2 primarily covers electronic transactions, it is important to consider the implementation of biometrics more broadly, to get the full benefits of an omni-channel solution across digital channels, the contact center and the physical branch.

How can Nuance help

Nuance biometrics solutions can help you meet PSD2 and SCA mandates, by strengthening the security of authentication and fraud prevention processes, while boosting customer experience and brand loyalty.

Companies need to find the right balance between three goals:

1. Optimize the customer experience and maximize the acceptance of genuine transactions.
2. Minimize fraud losses by detecting and rejecting fraudulent transactions while keeping false positives to a minimum.
3. Manage the operational costs of fraud management activities by automating fraud prevention operations and minimizing agents' workload with high quality fraud alerts.

On June 21, 2019, the European Banking Authority (EBA) published the validity of different biometrics[4] as an element within the “inherence” category, thus opening the door to implement sophisticated strong customer authentication procedures that are not dependent on possible security failures in communications infrastructures.

Nuance’s biometric solutions for customer authentication and fraud detection are powered by AI algorithms enabling fast and reliable authentication. Nuance provides multiple integrated biometric modalities, high accuracy, strong anti-spoofing and fraud detection. Additionally, a powerful risk engine enables real-time decisions based on various risk and familiarity signals. Nuance solutions build on many years of experience developing and delivering enterprise-class biometric engines that authenticate over 400 million customers around the world and are adopted by hundreds of organizations, including leading financial institutions globally.

Nuance biometric capabilities include:

Behavioral biometrics
Each person is unique in how they interact with their devices. Nuance Gatekeeper analyzes biometric behavior patterns including how fast a person types, hold their smartphone, the pressure and surface area of their fingers as they interact with their device or even how they pause when accomplishing a task. If these behaviors change, or if the behavioral pattern matches that of a potential fraudster, Nuance Gatekeeper can elevate the risk level associated with the transaction. Behavioral biometrics can be an ideal method to strengthen authentication and reduce fraud across web, mobile and chat channels while being completely invisible to the customer.

Voice biometrics
Among all biometrics, voice biometrics has reached a high level of maturity in recent years, with Nuance being the world leader in providing biometric technology solutions to the financial sector with more than 500 clients and 400 million voice prints.

Nuance’s voice biometrics technology is capable of generating a voice print after analyzing hundreds of attributes and physical characteristics of each individual (vocal tract, language, oral cavity, etc.) and characteristic of the voice, ensuring the verification of the speaker’s identity with an accuracy greater than 99%.

A voice print that can be used to identify the speaker both on a voice channel (IVR and Contact Center) and on digital channels (mobile app, web, email, social networks, etc.).

Facial recognition
The use of facial recognition has become more widespread, as it provides a seamless way for users to authenticate by leveraging the high-quality cameras available on most smart phone and tablet devices. Facial recognition can also act as a deterrent for fraudsters by limiting their ability to continue with their criminal activity when faced with a facial recognition authentication request. Nuance Gatekeeper provides facial recognition as one of the modalities you can use to secure customer authentication, with high levels of accuracy and liveness detection capabilities.

ConversationPrint
A form of behavioral biometrics, ConversationPrint™ is a true industry first and can identify fraudulent activity in real time based on a choice of words and patterns of speech or typed text during an interaction with a human or a virtual assistant across digital and contact center channels. By analyzing vocabulary, sentence structure, grammar, and more, ConversationPrint can enable continuous authentication during a conversation, such as in a chat session. It also provides a powerful way to detect fraud by recognizing conversation scripts that resemble patterns of a potential fraudster.

With multi-modal enterprise-class biometric capabilities powered by AI, Nuance can help your organization deliver Strong Customer Authentication to achieve your compliance objectives, while also optimizing the customer experience and reducing fraud across all customer interaction channels.

Nuance Intelligent Detectors

Intelligent Detectors provide risk signals that make identifying fraudsters much easier.

Liveness ID
Ensures the subject providing the biometrics is a human.

Synthetic ID
Detects even perfectly-rendered synthetic speech.

Playback ID
Detects when a fraudster is using a recording of their target’s voice.

Geo ID
Identifies the country and city the device is associated with.

Network ID
Analyzes network quality to detect suspicious changes.

Channel ID
Analyzes the full audio to determine the device type used during the interaction.

ANI ID
Analyzes the metadata in a phone call and determines when an incoming call is from a legitimate caller.

[4] “Inherence may include retina and iris scanning, fingerprint scanning, vein recognition, face and hand geometry, voice recognition”. European Banking Authority (21 June 2019)

Why Nuance?

Nuance Communications (NASDAQ: NUAN) is a multinational company with more than 30 years of experience in innovation, research, development and commercialization of biometrics solutions and voice and natural language understanding technologies based on Artificial Intelligence (AI). Today, many of Nuance's solutions are present in most of the customer service departments of a large number of multinational companies, adding value and helping to improve the experience and security of their customers.

Over 400 million individuals around the globe authenticate to customer care services with Nuance voice biometric solutions. So far this year, over 8 billion successful biometrics transaction have been processed without a single reported fraudulent authentication, saving $2B annual fraud.

Our customer references using Nuance biometrics solutions for customer authentication and fraud prevention include top leading banks and financial services companies, telcos, insurances, retailers, utilities and government companies around the world. Below are some examples of those customers who have authorized us to use their logo in public:

Manulife · BARCLAYS · Royal Bank of Scotland · Crédit du Nord

HSBC · ING · TalkTalk For Everyone · BBVA · ANZ

USAA® · Telefónica · Santander · بنك أبوظبي التجاري ADCB

Australian Government Australian Taxation Office · ROGERS™ · Eastern Bank · VIRGINIA Credit Union

LLOYDS BANK · Vanguard® · Deutsche Telekom · nab · TD

Learn more

Learn more about these and other security and biometrics solutions for customer authentication and fraud prevention by clicking here.

If you would like to request a product demo or you have any question please send an email directly to: pilar.blasco@nuance.com

About Nuance Communications, Inc.

Nuance Enterprise is reinventing the relationship between enterprises and consumers through customer engagement solutions powered by artificial intelligence. We aim to be the market leading provider of intelligent self- and assisted-service solutions delivered to large enterprises around the world. These solutions are differentiated by speech, voice biometrics, virtual assistant, web chat and cognitive technologies; enabling cross-channel customer service for IVR, mobile and web, Inbound and Outbound; and magnified by the design and development skill of a global professional services team. We serve Fortune 2500 companies across the globe with a mix of direct and channel partner selling models.