

Jaarverslag 2018

Bankieren met
de menselijke maat

1.4 ONTWIKKELINGEN IN DE SECTOR

OPENING FINANCIËLE SECTOR VERANDERT SPEELVELD VOOR BANKEN

De invoering van PSD2 zet de bancaire sector open voor nieuwe spelers. Onder deze Europese wetgeving kunnen andere partijen dan traditionele banken vergunningen aanvragen als betalingsinstelling. PSD2 verplicht banken om op verzoek van de klant betaaldata ter beschikking te stellen aan deze andere partijen. Op basis van deze data kunnen diensten en nieuwe verdienmodellen worden ontwikkeld. Dat biedt niet alleen mogelijkheden voor fintechs, maar ook voor de grote technologiebedrijven, die zeer bedreven zijn in het hanteren van data als verdienmodel. Deze BigTechs hebben reeds verschillende voorbereidende activiteiten ontplooid, vaak middels kredietverlening aan gebruikers van hun platformdiensten. In de Verenigde Staten is Amazon een grote kredietverstrekker aan verschillende bedrijven die op hun platform winkels hebben. Ook Facebook en Uber vervullen deze rol. De volgende te verwachten stap is het faciliteren en afhandelen van de voorkant van de betalingen.

Apple Pay en Google Pay bestaan al langere tijd, maar met de toekenning aan Google van de e-money licence in Ierland en PSD2-licenties in Litouwen, is de volgende stap dichterbij. Hierin schuilt dan ook een dreiging voor de bancaire sector. Google kan een grotere positie op de betaalmarkt verwerven als de onderneming, die al beschikt over contextuele data van klanten, zoals lokatiegegevens, dit binnenkort kan combineren met transactiegegevens en toestemming om betalingen te doen.

Verschillende online banken betreden de (internationale) markt. Het aantal klanten van deze banken laat een gestage groei zien. Daarnaast zien we de ontwikkeling waarbij bestaande banken zichzelf ontwikkelen tot nieuwe online banken (greenfield banken).

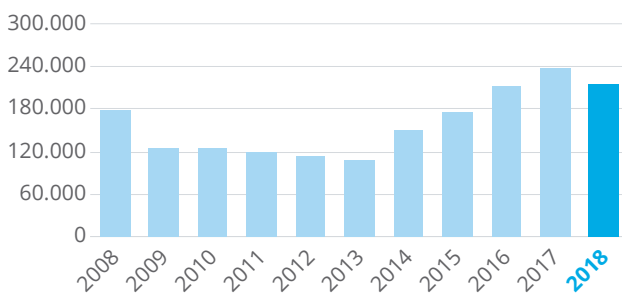
Toch draait het in de toekomst niet alleen om technologie. Juist als technologie niet meer de onderscheidende factor is, gaat het erom wat een bank kan toevoegen. 'Zachte' kerncompetenties als kennis, sociale vaardigheden en maatschappelijke betrokkenheid gaan dan een belangrijke rol spelen. Ook de mate waarin een bank zich weet te beschermen tegen cyberaanvallen (de digitale weerbaarheid van de bank) en in hoeverre de bank data beschermt zullen meespelen bij de keuze voor een bepaalde bank.

INVLOED VAN ARTIFICIAL INTELLIGENCE (AI)

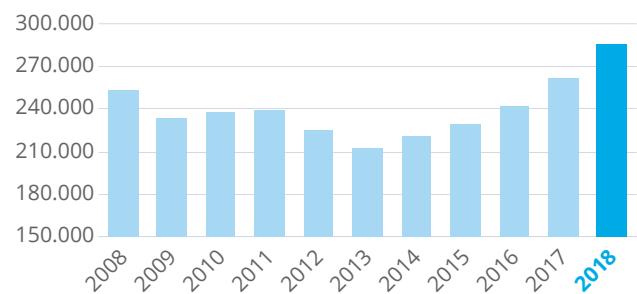
Professionals in de financiële sector verwachten dat door ontwikkelingen op het gebied van AI de branche in 2030 totaal is getransformeerd. Dat is te concluderen uit het onderzoek van Hays: 'Baan van de Toekomst: De financiële sector in 2030'.

Van de ondervraagden gelooft 88% dat al het betalingsverkeer dan realtime zal plaatsvinden. Zo bieden de meeste Nederlandse banken, waaronder ASN Bank, RegioBank en SNS, vanaf begin 2019 Instant Payments aan. Binnen een paar seconden geld overboeken naar of ontvangen van rekeningen bij andere banken is dan mogelijk voor meer dan 95% van alle bankrekeningen in Nederland. AI en big data

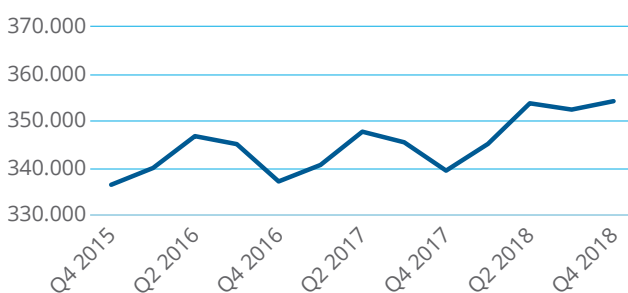
Aantal verkochte woningen



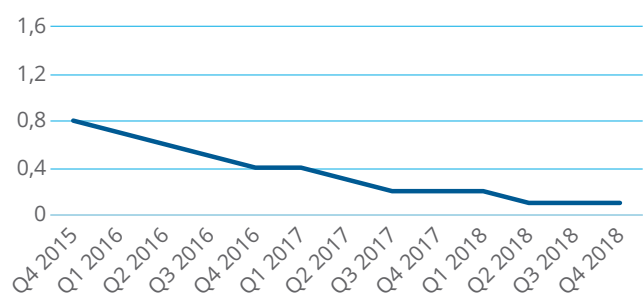
Gemiddelde verkoopprijs (In euro's)



Totaal spaargelden (in miljoenen euro's)



Gemiddelde spaarrente (in %) (opzegtermijn < 3 maanden)



vormen volgens 64% de basis van elke beslissing in de financiële sector van de toekomst.

De eerder genoemde toetreders zullen de rol van AI in de financiële sector alleen maar vergroten. AI, gevoed door een rijke set aan data (met dank aan PSD2), maakt het mogelijk dat klanten op eenvoudige wijze overzicht en inzicht in hun financiële situatie krijgen. Vervolgens kunnen slimme modellen de klant helpen de juiste beslissingen te nemen om hun financiën optimaal te managen. De verwachting is dat dit over de volle breedte van het financiële domein zal gebeuren. Veel toepassingsmogelijkheden zijn gericht op het verhogen van de klantbeleving en snellere analysemogelijkheden, zoals bij het verstrekken van een hypotheek. Wij zien het grote technologische potentieel van AI als belangrijk hulpmiddel om onze missie Bankieren met de menselijke maat te versterken.

CYBERDREIGING BLIJFT ONVERMINDERD HOOG

De dreiging van cybercrime voor de Nederlandse financiële sector is permanent, aanzienlijk en blijft zich ontwikkelen. Cyberaanvallen zijn profijtelijk, laagdrempelig en weinig riskant voor aanvallers. Aanvallers richtten zich in het verleden vooral op klanten van financiële instellingen. Nu vallen cybercriminelen steeds vaker financiële instellingen aan, waarbij aanvalsmethoden geavanceerder worden. Ook kunnen meerdere instellingen gelijktijdig doelwit zijn, zoals de DDoS-aanvallen op de grootbanken in begin 2018 hebben laten zien. Het Financieel Stabiliteitscomité waarschuwt voor dit risico op geavanceerde cyberaanvallen waarbij de financiële stabiliteit in het geding kan komen. Ook het Nationaal Cyber Security Centrum¹ (NCSC) waarschuwt dat de gevolgen van aanvallen en uitval groot en zelfs maatschappij-ontwrichtend kunnen zijn.

De schade door fraude in het betalingsverkeer in Nederland is, voor het eerst na een jarenlange daling², gestegen. De stijging manifesteerde zich bij internetbankieren en bij fraude met gestolen of verloren betaalpassen. Naast het behalen van financieel gewin en het verstoren van de dienstverlening, is diefstal van gegevens een steeds vaker voorkomend doel van cybercriminelen.

Het verhogen van de veiligheid in het digitale domein is een topprioriteit voor de overheid. Ook de DNB heeft in toenemende mate aandacht voor cybersecurity: er is een meldplicht voor cyberincidenten en jaarlijks wordt de cyberweerbaarheid van de financiële sector getest middels Threat Intelligence Based Ethical Red Teaming (TIBER)³. Concluderend blijft de noodzaak te investeren in onze digitale veiligheid onverminderd hoog. Daarnaast is interbancaire en publiek-private samenwerking noodzakelijk om de cyber weerbaarheid duurzaam te blijven verhogen.

BELANG VAN DATA EN PRIVACY GROEIT

De automatisering en digitalisering van de financiële dienstverlening gaan steeds verder. Daarbij wordt data en vooral de bescherming van dan wel controle over data steeds belangrijker. Wetgeving heeft daarbij in 2018 een belangrijke rol gespeeld. De Europese verordening 'Algemene verordening gegevensbescherming (AGV)' is ingevoerd en heeft bijgedragen aan een toenemend bewustzijn van de consument over het belang van privacy bij het gebruik van data. De wet die in Nederland als AVG door het leven gaat, geeft de consument ook rechten om gegevens in te zien of gegevens te laten verwijderen.

Het privacybewustzijn is verder versterkt door de discussie rond de Wet op de Inlichtingen en Veiligheidsdiensten (de zogenaamde Sleepwet). Daarnaast maakt het Cambridge Analytica schandaal duidelijk dat gratis gebruik van diensten als Facebook ook z'n keerzijde heeft.

Ook bij PSD2 speelt een privacy discussie, aangezien een betaaltransactie altijd twee partijen kent (betaler en ontvanger). Als de betaler zijn betaaldata deelt gaan onbedoeld ook gegevens mee van de ontvangende partij.

In deze nieuwe situatie is het van het grootste belang om de consument bewust te maken van mogelijkheden en gevaren. Want hoewel data de kern vormt van het moderne bankieren, blijft de klant altijd eigenaar van zijn data en moet de klant in staat worden gesteld om regie te voeren over zijn data en het gebruik van zijn data.

De Volksbank onderkent dat belang vanuit het Bankieren met de menselijke maat en heeft dat vertaald in een Datavisie: hoe wij omgaan met Data & Privacy en hoe wij de klant op dat gebied willen ondersteunen.

Klanten vertrouwen ons al meer dan 200 jaar hun geld toe. Wij vinden dat zij dit ook met hun persoonlijke data moeten kunnen. In dat kader hebben wij in de Datavisie duidelijk kaders gesteld aan hoe wij, in deze snel veranderende financiële wereld, Data & Privacy vertalen naar Bankieren met de Menselijke Maat. Voor ons is de klant altijd eigenaar van zijn data, zullen we nooit data aan andere partijen verkopen en gebruiken we de data van de klant alleen met zijn toestemming en altijd in dienst van zijn eigen Financiële Onbezorgdheid.

We zijn er van overtuigd dat een groeiend aantal consumenten behoefte heeft aan bank die volledig te vertrouwen is in het gebruik van klantdata. Die privacy hoog in het vaandel heeft en de klant helpt en beschermt. Want we kunnen de mogelijkheden van technologie alleen maar ten volle benutten als de klant vertrouwen heeft in ons als organisatie en in de wijze waarop wij verantwoord met data en privacy omgaan.

¹ Cybersecuritybeeld Nederland (CSBN) 2018, een jaarlijkse publicatie van NCSC (<https://www.ncsc.nl/>)

² Betaalvereniging Nederland (<https://www.betalvereniging.nl/>)

³ TIBER-NL goes Europe (<https://www.dnb.nl/>)