Kennisgroep Betalingsverkeer stelt zich voor

Actuele ontwikkelingen en risico's in het betalingsverkeer

3 december 2020

In de NOREA-webinar van 8 oktober 2020 presenteerde de kennisgroep Betalingsverkeer haar visie op ontwikkelingen in het betalingsverkeer. Tijdens dit webinar gaven de deelnemers via de tool 'Wordle' aan welke ontwikkelingen zij in het werkveld zien. Figuur 1 geeft daar een impressie van.

Figuur 1: Weergave relevante ontwikkelingen volgens de meer dan 200 webinardeelnemers

In dit artikel vind je een overzicht van de ontwikkelingen die wij als kennisgroep betalingsverkeer zien. Deze ontwikkelingen zijn relevant voor IT-auditors die te maken hebben met betalingsverkeer vanwege de impact op hun werkzaamheden.

Er zijn snelle, ingrijpende ontwikkelingen gaande in het betalingsverkeer, waardoor ook het werkveld van de IT-auditor verandert. Hier bespreken we deze ontwikkelingen globaal.

Wil je meer weten, of ben je geïnteresseerd om bij te dragen aan de kennisgroep, neem dan contact met ons op.
Je kunt ons benaderen via norea@norea.nl of via ons twitteraccount @PaymentFriends.

We behandelen de volgende ontwikkelingen met de bijbehorende risico's:

- Nieuwe partijen, afzetkanalen en regelgeving
- Verdienmodellen
- Toename van externe standaarden
- Legacy-systemen
- Klassieke risico's rond general controls
- Payment Services Directive 2 (PSD2)
- COVID-19

Bij elk van deze onderwerpen geven we de IT-auditor een aantal tips.

We sluiten ons artikel af met enkele tips om het hoofd te bieden aan de toenemende complexiteit van het betalingsverkeer.

Ontwikkeling 1: Nieuwe partijen, afzetkanalen en regelgeving

De volgende vier drivers bepalen sterk de huidige ontwikkelingen van het betalingsverkeer in de retail:

- Technologische ontwikkelingen
- Wet- en regelgeving, denk bijvoorbeeld aan PSD2 (zie 'Ontwikkeling 6')
- De opkomst van techbedrijven
- Veranderend gedrag van de gebruikers

Deze ontwikkelingen leiden ertoe dat het betalingsverkeer, dat traditioneel door de banken en *card schemes* werd aangeboden, verandert. Banken overwegen of zij hier een positie in kunnen of willen behouden en nieuwe toetreders zien kansen om een nichemarkt te bedienen of met nieuwe technologie een aanzienlijk deel van de betaalmarkt in te nemen.

We zien de volgende drie ontwikkelingen voor de toekomst van het betalingsverkeer in de retail:

1. Bestaande betaaldienstverleners, zoals de traditionele banken, bieden nieuwe betaalmethoden aan, eventueel door overname van of partnerships met andere betaaldienstaanbieders.
2. Fintechbedrijven, zoals Adyen, ontwikkelen hun eigen gespecialiseerde betaalfunctie en bieden die aan.
3. Techbedrijven, zoals Apple en platforms, vullen een groot deel van de betaalketen in.

Het aanbod van betaalmethoden is sterk toegenomen. Ook zien we meer en meer cryptovaluta's. Bovendien verschuift het betaalgedrag van de consument van cash naar card-based en naar mobiel en contactloos betalen. Verder zijn de betaalketens diverser en complexer geworden. Steeds meer partijen vervullen een rol in de betaalketens en zullen moeten bijdragen aan de goede werking van het betalingsverkeer als geheel. Bovendien spelen, naast de banken, ook andere betaalinstellingen, techbedrijven, platformen, en telco's in toenemende mate een rol in de betaalkanalen en -ketens.

De nieuwe activiteiten van toetredende partijen vallen niet altijd onder bestaande wet- en regelgeving. Dit gat wordt gretig gebruikt door een aantal techbedrijven, terwijl de traditionele instellingen nog de last van bestaande, strenge wet- en regelgeving met zich meedragen. Hierbij speelt onder andere de vraag of zij als techbedrijf of als financiële instelling moeten worden gezien. Deze onduidelijkheid is een nadeel voor de bestaande organisaties die al als financiële instelling zijn bestempeld, en een voordeel voor de nieuwe toetreders. Die presenteren zich vaak als techbedrijf, waardoor ze niet hoeven te voldoen aan de wet- en regelgeving voor financiële instellingen.

Onder PSD2 zien we dat organisaties steeds meer met elkaar samenwerken, diensten aan elkaar uitbesteden en toegang tot elkaars IT-omgeving krijgen. Dit alles ontslaat organisaties echter niet van de verantwoordelijkheid die wet- en regelgeving heeft opgelegd. De organisatie is dan ook verplicht vast te stellen of de andere organisaties waarmee men samenwerkt zich aan alle gemaakte afspraken houden. Elke organisatie in de betaalketen is en blijft immers zelf eindverantwoordelijk.

IT-auditors hebben diverse mogelijkheden om over andere organisaties zekerheid (*assurance*) over de naleving van afspraken te krijgen. Zowel de Algemene Verordening Gegevensbescherming (AVG) (artikel 28: verwerkersovereenkomsten), als PSD2 (European Bankers Association's 'Regulatory Technical Standards – RTS – on strong customer authentication and common and secure communication under Article 98 of Directive 2015/2366'), als ISO 27002 (hoofdstuk 15: leveranciersrelaties) geven handvatten voor hetgeen moet worden geregeld. Denk aan service level-rapportages, ISAE 3402-rapporten, ISO 27001-certificering, technische en organisatorische maatregelen, afspraken met subverwerkers, *right to audit* en afhandelen van (security-)incidenten en datalekken. IT-auditors kunnen toezichthouders helpen nieuwe wet- en regelgeving om te zetten naar control frameworks met maatregelen waar organisaties aan moeten voldoen.

Tips voor de IT-auditor

- IT-auditorsorganisaties helpen wet- en regelgeving te interpreteren, intern de governance op orde te brengen en audits van toezichthouders te begeleiden.
- Bij samenwerking of uitbesteding kunnen IT-auditors de dienstverlenende organisatie helpen naleving van afspraken aan te tonen.
- Ook kan een IT-auditor de uitbestedende organisatie helpen bij het interpreteren en controleren van de ontvangen rapportages om vast te stellen of de afspraken daadwerkelijk voldoende zijn nageleefd en welke restrisico's er nog zijn.

Ontwikkeling 2: andere verdienmodellen en rol van de banken

Een bank verdient vooral aan interest en opbrengsten voor verrichte transacties. Het verdienmodel gebaseerd op de *Net Interest Margin* (NIM) staat onder druk: geld tegen een bepaalde interest aantrekken (bijvoorbeeld spaarrekening) en tegen een hogere interest uitzetten (bijvoorbeeld hypotheek). Het verschil tussen deze interestpercentages is al lange tijd klein. Ook betaalrekeningen zijn daardoor minder winstgevend. Het niet langer aanbieden van dit product is geen optie want een betaalrekening is het startpunt voor hypotheken, verzekeringen, beleggingen en andere producten (cross-selling).

De ontwikkeling om een product te beprijzen in overeenstemming met de gemaakte kosten, zien we ook terug in het betalingsverkeer. Al jaren worden geen gratis betaalrekeningen meer aangeboden en de kosten van een betaalpakket worden in lijn met de kosten gebracht, of de klant wordt een goedkoper alternatief aangeboden. Bijvoorbeeld: elektronisch bankafschrift is gratis, maar gebruik van papieren afschrift kost geld.

Voor de financiële crisis waren veel banken op het overnamepad en 'knoopten' vervolgens de eigen en de overgenomen IT-systemen 'aan elkaar'. Er was geen noodzaak te standaardiseren: er was geld in overvloed. Veel van deze systemen zijn geschreven in oudere talen die inmiddels hun functionele levensduur ruim hebben overschreden. Onderhoud wordt steeds lastiger doordat het aantal mensen dat de computertaal beheerst, afneemt. Door onvoldoende goede kwaliteitdocumentatie is men terughoudend onderhoud te plegen – dit geldt ook voor opheffen van bestaande functionaliteit en aanbieden van nieuwe functionaliteit via smartphones. Want: 'als ik hier trek, gaat heel ergens anders dan verwacht ook iets bewegen'. Ook gebruiken banken nog fysieke ('*brick and mortar*') kantoren tegen hoge huurprijzen en met hoge personeelskosten.

Nieuwkomers in de markt dagen de traditionele banken en hun betalingsverkeerprocessen, technologie en verdienmodellen uit. Zij kunnen gebruikmaken van modernere computertalen, bieden alleen virtuele producten en de meer winstgevende producten aan. Hierdoor kunnen zij producten tegen lagere kosten aanbieden.

Nieuwkomers komen vooral uit de hoek van de techbedrijven en de telco's, die aanvullende producten bieden op hun initieel core product-browser of smartphone.

Daarnaast verwacht de klant altijd en overal te kunnen bankieren, wat de banken dwingt volledig digitaal te gaan: 24×7 op elk medium (laptop, telefoon, et cetera) tegen zo laag mogelijke kosten. Automatisering, robotisering en kunstmatige intelligentie worden ingezet om aan de steeds veeleisendere klant tegemoet te komen. Financiële instellingen presenteren zich minder als bank, en meer als een platform waar bedrijven, organisaties en particulieren graag vertoeven en waar je kan betalen, sparen of beleggen.

PSD2 stimuleert dit alles. Als klanten toestemming verlenen, kan data worden gedeeld en inzicht worden verkregen. Dit geldt zowel voor de klant ('hoe besteed ik mijn maandelijks inkomen') maar ook voor de financiële nieuwkomers ('welk product kan ik de klant op basis van zijn bestedingsgedrag aanbieden').

Samenwerking biedt ook manieren om kosten te besparen. Dit kan onder meer door samen te werken met soortgelijke organisaties. Bijvoorbeeld niet langer zelf geldautomaten aanbieden en beheren, maar dit samen doen met andere banken onder het neutrale label 'Geldmaat'. Ook is samenwerking mogelijk buiten de financiële sector. Een voorbeeld is de 'digitale betalingsmachtiging', die het makkelijker maakt op moment van aankoop in de winkel digitaal af te rekenen via een incasso.

Tips voor de IT-auditor

- Valideer of producten passen binnen de strategie van de bank en of de producten en de bijbehorende processen efficiënt in gebruik zijn.
- Zorg dat je up-to-date blijft met nieuwe ontwikkelingen en de impact daarvan en help de organisatie deze te vertalen naar de bedrijfsstrategie.

Ontwikkeling 3: Toename van externe standaarden

De ontwikkelingen in de financiële markten laten zien dat de bestaande wet- en regelgeving kansen biedt aan diverse toetreders om nieuwe activiteiten te starten. Dit dwingt veel partijen die in het betalingsverkeer een rol spelen om met nieuwe wet- en regelgeving, eisen, frameworks of standaarden te komen. Deze behoefte helpt niet alleen de wetgever, toezichthouders of de centrale banken maar biedt de betrokken partijen onderling en daarmee de gehele keten van betalingsverkeer meer zekerheid. Dit alles moet ertoe leiden dat de gebruikers, zowel particulieren als organisaties, vertrouwen houden in het betalingsverkeer als stelsel.

De behoefte aan nieuwe eisen en richtlijnen leidde tot het volgende nieuwe pakket van eisen aan organisaties in de financiële markten:

- SWIFT heeft het Customer Security Controls Framework (CSCF) geïntroduceerd. Dit verplicht SWIFT-gebruikers om een self-assessment uit te voeren. SWIFT kan de resultaten delen met toezichthouders en tegenpartijen.
- Creditcard-uitgevende instellingen (issuers), financiële instellingen die de cards verstrekken (acquirers) en bedrijven die creditcardtransacties gebruiken en verwerken (merchants) moeten gebruikmaken van serviceproviders die compliant zijn met industry data security standards. Voorbeelden van zulke standaarden zijn de Payment Card Industry Data Security Standard (PCI DSS), PCI PIN en landspecifieke security-eisen. Issuers, acquirers en merchants zijn aanspreekbaar voor incidenten door non-compliance.
- Wanneer een klant er op de website van een acceptant voor kiest om zich te identificeren met of in te loggen met iDIN, wordt hij doorgestuurd naar een beveiligde iDIN-webpagina van zijn eigen bank. Betaalvereniging Nederland stelt eisen aan aanbieders van iDIN.
- Met PSD2 kunnen klanten nieuwe online betaal- en rekeningdiensten gaan gebruiken. Hiervoor is het nodig dat klanten een derde partij (een andere financiële instelling) toegang geven tot hun betaalrekening bij hun bank. Europese wetgeving en standaarden geven hier richting aan.
- *Money Laundering* (ML, witwassen) is het uitvoeren van transacties waarmee illegaal verkregen gelden worden omgezet naar gelden in de legale betaalketen, waarmee de bron van deze illegaal verkregen gelden wordt. Toezicht op uitvoering van de Wet Financieel Toezicht (Wft) is strenger geworden om te voorkomen dat witwassen (Anti Money Laundering – AML) en/of terrorisme financiering gefaciliteerd wordt. Zie over AML ook het verslag in dit blad van het event dat de NOREA & ISACA YoungProfs op 18 februari 2020 organiseerden: 'Anti Money Laundering in a digital world'.

Tips voor de IT-auditor

De IT-auditor kan organisaties helpen om:

- te voldoen aan de al maar toenemende wet- en regelgeving;
- de nieuwe wet- en regelgeving, eisen, frameworks of standaarden om te zetten naar begrijpelijke taal voor de organisaties, om te kunnen aantonen dat ze aan de gestelde eisen voldoen;
- een normenkader te ontwikkelen, zodat zij andere partijen in het betalingsverkeer kunnen aantonen compliant te zijn. Een goed voorbeeld is de PSD2 Guidance van onze kennisgroep, samen met de Betaalvereniging Nederland, de Nederlandse Vereniging van Banken en enkele grootbanken.

Ontwikkeling 4: Legacy-systemen

'De wet van de remmende voorsprong' is een uitdrukking die zeker geldt voor sommige IT-systemen in de financiële sector. Banken en verzekeraars waren vaak koploper in de eerste automatiseringsgolf in de jaren zeventig en tachtig van de vorige eeuw in Nederland, maar nu lopen de nieuwe toetreders voorop.

Net als sommige grote uitvoeringsorganisaties van de rijksoverheid, hebben banken en verzekeraars in bovengenoemde periode via eigen systeemontwikkelingsafdelingen relatief snel IT-systemen ontwikkeld. Deze waren vaak geschreven in derde generatie-programmeertalen als Cobol. Deze systemen konden snel en zeer betrouwbaar grote gegevensbestanden verwerken.

Kwaliteiten als betrouwbaarheid en de verwerking van grote gegevensbestanden hebben er mede voor gezorgd dat veel bedrijven lang hebben vastgehouden aan deze IT-systemen. Vaak te lang: bij sommige bedrijven is het gebruik van deze IT-systemen inderdaad zo lang geweest, dat het heeft geleid tot verouderde IT-systemen (*legacy*).

Als een organisatie tot het besef is gekomen dat wellicht legacy-systemen in bedrijf zijn, is men vaak geneigd te geloven in het standaardbeeld van legacy-systemen, namelijk: hoge onderhoudskosten, slechte onderhoudbaarheid en lange *time-to-market* van nieuwe producten of diensten. Dan wordt meestal zonder onderzoek hals over kop een vernieuwingsprogramma opgestart, zonder te kijken naar de andere, positieve kwaliteiten van deze systemen. De legacy-systemen hebben zich vaak bewezen: ze zijn stabiel en relatief goedkoop. Vaak zijn de veronderstelde hoge onderhoudskosten niet gebaseerd op feiten.

In de literatuur wordt dan ook de volgende aanpak voorgesteld.1

- Voor de juiste keuze tussen nieuwbouw en onderhoud van legacy is tijdig en gedegen onderzoek naar kwaliteit van de software nodig.
- Maak heldere afspraken over de definities over kwaliteit en ontwikkelkosten.

Tips voor de IT-auditor

- Ga na of de organisatie al een kwaliteitsonderzoek naar software heeft uitgevoerd, met daarbij vooral duidelijke definities van onderhouds- en ontwikkelingskosten en kwaliteit.
- Stel vast of de organisatie een gedegen beleid heeft voor *software life cycle management* (SLM) of *application life cycle management* (ALM) en een programma met bijbehorende projecten heeft. Als er geen SLM- of ALM-programma is, dan moet de IT-auditor in samenspraak met de verantwoordelijke accountant hier een opmerking over opnemen in de verslaglegging. Is er wel een SLM- of ALM-programma, dan moet de IT-auditor periodiek de uitvoering en voortgang daarvan onderzoeken. Bij de Belastingdienst loopt bijvoorbeeld een SLM-project, en de Auditdienst Rijk rapporteert jaarlijks over de uitvoering ervan.

Ontwikkeling 5: klassieke risico's rond general controls

Een bedrijf in de financiële sector heeft te maken met vele technologische ontwikkelingen, zoals wel of niet overgaan naar de cloud. Bij alle ontwikkelingen is er één onderwerp waar altijd aandacht voor moet blijven: de risico's op het gebied van *general IT controls* zoals toegangsbeveiliging, change management en continuïteitsmaatregelen.

Wanneer bijvoorbeeld een systeem voor betalingsverkeer naar de Cloud is gemigreerd, is vanwege de cyber security-risico's extra aandacht nodig voor de toegangsbeveiliging. Ook veroorzaken nieuwe kanalen en spelers in de financiële sector fragmentatie van systemen in de sector. In dit geval is de vraag hoe beschikbaarheid kan worden gegarandeerd extra nadrukkelijk aan de orde. Verder komt bij nieuwe ontwikkelmethodieken zoals agile en het werken met DevOps bijvoorbeeld de vraag op hoe het change managementproces moet plaatsvinden.

Tips voor de IT-auditor

- Verlies de general IT controls niet uit het oog bij de invoering van nieuwe ontwikkelingen. Blijf aandacht besteden aan de general IT controls, application controls in het systeem en de procedurele beheersmaatregelen eromheen.
- Specifiek voor cloud- en ketenoplossingen:
    - heb aandacht voor (onder)aannemers en de beheersmaatregelen die geregeld zijn; denk bijvoorbeeld aan effectief gebruik van assuranceverklaringen ISAE3402, SOC2/3000D).
    - Indien men op zoek is naar assurance in de keten: waar liggen de grenzen van de keten?

Ontwikkeling 6: nieuwe wetgeving rond PSD2 en beschikbaar normenkader

Met de invoering van PSD2 zijn de eisen van de Europese Unie voor het beschikbaar maken van betalingsdata en voor beveiliging aangescherpt. PSD2 vraagt van marktpartijen die betalingsverkeer aanbieden ('account service payment servicing providers' ofwel banken en andere organisaties die betaaldiensten aanbieden) om via hun systemen aan *trusted third parties* (TTPs) de mogelijkheid te bieden betalingen voor klanten te faciliteren en accountinformatie op te vragen. Dit uiteraard alleen als de klant hiermee instemt (*consent*) en TTPs zijn goedgekeurd door de ECB/DNB. Ook stelt PSD2 eisen aan klantauthenticatie (*two-factor authentication*), vastgelegd in regulatory technical standards. De PSD2-wetgeving geeft ook eisen voor reviewactiviteiten (in 'artikel 3') en vraagt vooral om het documenteren, testen, evalueren en – de auditor spitst de oren – het auditen van onderliggende processen en infrastructuur. Omdat de wetgeving ruimte laat voor interpretatie, heeft de kennisgroep Betalingsverkeer van NOREA samen met de Betaalvereniging Nederland, de Nederlandse Vereniging van Banken en enkele grootbanken praktische guidance uitgewerkt voor auditors. Met de bijbehorende control matrix krijg je grip op PSD2.

Tips voor de IT-auditor

- Bestudeer de practical guidance op de NOREA-site.
- Houd actuele ontwikkelingen bij (regelgeving beweegt).
- Benader NOREA of de kennisgroep Betalingsverkeer als je behoefte hebt aan verdieping.

Ontwikkeling 7: COVID-19

Ook wij kunnen het niet negeren: COVID-19 heeft ook impact op het betalingsverkeer. Cash-betalingen verminderen in razendsnel tempo omdat winkels vanwege besmettingsrisico's geen geld willen aannemen, en klanten er niet mee willen betalen. De bestaande trend waarbij online en pinbetalingen een steeds groter aandeel van het betalingsverkeer vormen, is daardoor drastisch versneld. Daarnaast worden limieten aangepast om het touch-based gebruik van pinautomaten zo laag mogelijk te houden. Specifieke risico's als *CxO*-fraude en *phishing*, maar ook risico's in operationele betalingsverkeerprocessen nemen toe doordat mensen meer *standalone* werken.

Tips voor de IT-auditor

- Voer specifieke risicoanalyses uit op de impact van COVID-19.
- Informeer je via de sites van DNB en NOREA regelmatig over actuele ontwikkelingen en aanbevelingen voor auditors.

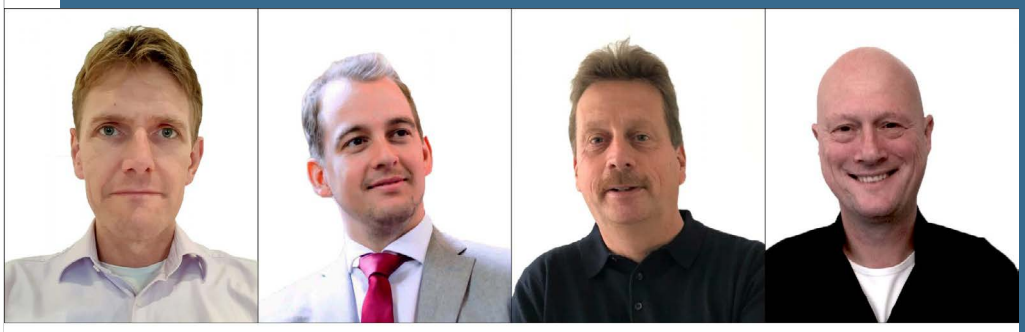
Afsluitende tips

In dit artikel hebben we laten zien dat het betaallandschap de laatste jaren een stuk complexer is geworden. We sluiten af met de volgende tips om aan die complexiteit het hoofd te bieden:

- Zorg voor voldoende capaciteit en deskundigheid op het terrein van betalingsverkeer.
- Bepaal of de *risk appetite* en de risicoanalyse voor het betalingsverkeer actueel zijn en of deze rekening houden de nieuwe ontwikkelingen.
- Bepaal of de maatregelen toereikend zijn voor de toenemende complexiteit van de betaalketens.
- Voer periodiek een audit uit in het inherent hoge risicogebied van het betalingsverkeer.
- Houd actuele ontwikkelingen bij.
- Benader NOREA of de kennisgroep Betalingsverkeer als je behoefte hebt aan verdieping.

De kennisgroep Betalingsverkeer

Dit artikel is een product van de kennisgroep Betalingsverkeer van NOREA. De kennisgroep produceert guidance en achtergronddocumenten en organiseert en seminars op het gebied van betalingsverkeer. Leden van de kennisgroep zijn:



Lodewijk Benjaminse | Willian Crielaars | Léon Dirks | Hans Koster

Wandena Punwasi | Erus Schuurman | Frank Waatjes

De kennisgroep is te bereiken via norea@norea.nl of via ons twitteraccount @PaymentFriends

Recente activiteiten zijn:

- Webinar 'Risico's van betalingsverkeer en PSD2';
- Handreiking auditaanpak PSD2;
- Factsheet overview PSD2

Literatuur

Banken.nl. *Bankensector.*

Ellen Klijnstra. *Anti Money Laundering in a Digital World; NOREA & ISACA Young Prof Event.*

European Banking Authority. *EBA publishes revised Guidelines on outsourcing arrangements.*

Hans Koster and Tom van de Ven. *Practical guidance for Internal Auditors on the annual audit of PSD2 related to strong customer authentication and common and secure communication.* NOREA.

Kennisgroep Betalingsverkeer. NOREA.

NOREA. *Payment Services Directive (PSD2).*

NOREA. *PSD2 Practical guidance Worksheet MVP 1-1.*