*BankID-bedrägeriet**

1. Inledning

Tiden då man gick till banken för att utföra sina bankärenden är för de flesta av oss sedan länge passerad. Idag hanterar man det mesta själv med hjälp av internet och digitala lösningar. Eftersom de tekniska lösningarna blivit ständigt säkrare och mindre utsatta för yttre påverkan har bedrägerierna som utnyttjar den enskilda människan som systemets svaga länk ökat.[1] Den 21 juni 2022 meddelade Högsta domstolen dom *i mål T 4623-21 (BankID-bedrägeriet)*, och lämnade med det ett efterlängtat prejudikat avseende konsumenters ansvar för obehöriga transaktioner, när transaktionen möjliggjorts av konsumenten själv i samband med att denna utsatts för ett förslaget bedrägeri. Mer specifikt handlade målet om gränsdragningen mellan grovt vårdslöst och särskilt klandervärt beteende enligt 5 a kap. 3 § betaltjänstlagen (2010:751).

Omständigheterna i målet kan i korta drag beskrivas enligt följande. En bankkund hade utsatts för ett telefonbedrägeri under vilket han lurades att medverka till att en bedragare kunde upprätta ett nytt mobilt BankID i kundens namn, vilket bedragaren sedan, och utan kundens vetskap, hade använt till att föra över sammanlagt 397 000 kronor från kundens konto.[2] Det sätt på vilket kunden medverkade var, förutom att på annans begäran använda sitt BankID och sin bankdosa för att legitimera sig, att han hade gett ut åtminstone en svarskod från bankdosan till bedragaren.

Eftersom det nya BankID:et hade använts av bedragaren var det enighet mellan parterna i tvisten om att transaktionerna var att anse som obehöriga i betaltjänstlagens mening och att den kontoförvaltande banken därför som utgångspunkt var skyldig enligt 5 a kap. 1 § betaltjänstlagen att återställa kundens konto. En banks skyldighet att återställa kontot begränsas emellertid enligt 5 a kap. 2 och 3 §§ betaltjänstlagen om de obehöriga transaktionerna har möjliggjorts genom att kunden brustit i att skydda sitt betalningsinstrument. Hur stor del av förlusten som kunden själv måste svara för beror på hur allvarligt kundens åsidosättande har varit, och i detta fall alltså om kundens beteende var att anse som grovt vårdslöst, vilket kunden själv erkänt, eller även som *särskilt klandervärt*.

Tingsrätten kom fram till att kunden inte hade agerat särskilt klandervärt, vilket ledde till att ansvaret begränsades till 12 000 kronor. Hovrätten bedömde

* Tack till forskningsamanuens jur.stud. Ludwig Irveland för hjälp med korrekturläsning.

1 Se Kjørven, Who pays when things go wrong? Online Financial Fraud and Consumer Protection in Scandinavia and Europe, European Business Law Review 31, no. 1 (2020) s. 77–110 på s. 78 med vidare hänvisningar.

2 Se p. 5 och 6 i HD:s domskäl.

frågan annorlunda och ålade kunden ett obegränsat ansvar för de genomförda obehöriga transaktionerna. HD gick på tingsrättens linje, och biföll kundens talan vilket även innebar att kunden befriades från skyldigheten att betala bankens rättegångskostnader i tings- och hovrätt.

Avgörandet är intressant av flera skäl. *För det första* innebär det något av en kursändring jämfört med hur många ansvarsbedömningar i ARN- och underinstanspraxis hittills sett ut, både i resultat och tillvägagångssätt för bedömningen. *För det andra* ger avgörandet välbehövlig ledning på ett område av mycket stor betydelse för både finansnäringen och konsumenter där många gränsdragningar hittills varit osäkra. Det är talande att instanserna, trots att samma omständigheter lagts till grund, hamnade i olika slutsatser och att hovrätten och HD hamnade i olika slutsatser fastän domstolarnas beskrivningar av rättsläget och de relevanta källorna inte skiljer sig åt på något väsentligt sätt.[3]

Fastän avgörandet kan anses utgöra något av en kursändring, framstår *resultatet* inte som oväntat eller överraskande. HD lade sig i domskälen rätt så nära uttalanden i förarbetena som, om än utan att gå in på de mer konkreta frågorna som rör just *e-legitimation* som betalningsinstrument,[4] ger ledning avseende tröskeln för kundens ansvar.[5] Trots att utgången i målet både kunde sägas vara väntad och efterlängtad, finns det mycket kvar att säga om avgörandet.

Det finns anledning att börja med en observation om något som även påverkat den följande strukturen på denna kommentar. Avgörandet är utformat som man nuförtiden ofta ser från HD, med en tydlig pedagogisk ambition med relativt omfattande beskrivningar av relevanta regler och källor och att möda lagts på att slå fast en allmän rättsregel, som sedan tillämpas i det konkreta fallet.[6]

[3] Se Svea hovrätts dom i mål T 8893-20 på s. 7 och 8 och jämför med HD:s beskrivning i p. 23–25.

[4] Förarbetenas exemplifiering tar sin utgångspunkt i att betalningsinstrumentet i fråga är ett kontokort och att kunden varit oförsiktig med kontokortet som sådant och/eller den till kontokortet kopplade personliga koden. Obehöriga transaktioner med kontokort förutsätter oförsiktighet hos kunden, att kunden lurats lita på en falsk webbplats eller att den tekniska utrustningen i en bankomat eller liknande modifierats, men däremot normalt inte att kunden genom ett bedrägeri lurats ge ifrån sig sitt kontokort eller sina behörighetsfunktioner.

[5] På området finns ett stort antal avgöranden, särskilt från ARN, som visar att förarbetsuttalandena om lagstiftarens intentioner inte i någon större omfattning verkar ha lagts till grund för rättstillämpningen. Martinson redovisar i kap. 10 och 11 i boken Femton förmögenhetsrättsliga forskningsresultat (2018) hur lagstiftarens intentioner avseende ansvarsfördelningen mellan konsument och betaltjänstleverantör avseende kontokort och tröskeln grov vårdslöshet kommit till uttryck under de senaste femtio åren och hur intentionerna att i större utsträckning skydda konsumenten inte uppnåtts genom ARN:s praxis, utan att praxisen istället bygger på typiserade bedömningar som överlag blir stränga mot konsumenten. I kap. 11.5 på s. 254 f. identifierar han flera tänkbara orsaker till diskrepansen mellan lagstiftarens intentioner och det praktiska utfallet av regeltillämpningen.

[6] Formuleringen har inspirerats av Lindskogs tillägg för egen del i NJA 2012 s. 535, referatet s. 553 (p. 3 i tillägget): ”Det framstår emellertid enligt min mening som klart att de högsta domstolarna med tiden har tagit på sig ett större ansvar för rättsbildningen. Detta gäller till att börja

Att omsorg lagts på att formulera en allmän rättsregel just i detta fall, framträder särskilt tydligt genom att HD verkar ha velat operationalisera kriteriet ”särskilt klandervärt” genom att formulera två olika bedömningsgrunder med tydlig regelstruktur och rekvisitliknande beståndsdelar för två huvudsakliga typfall där personliga behörighetsfunktioner kommit till en obehörig persons kunskap. Därtill angav HD ytterligare moment för hur bedömningen ska gå till och identifierade även faktorer som kunde förväntas vara av särskilt stor betydelse. Det handlar alltså om en lagtolkning, men där de preciserande förklaringarna fått utformning som regler med rekvisit.[7] När det sedan kommer till bedömningen i det konkreta fallet, blir det dock otydligt i vilken mån som den tidigare uppställda regeln verkligen tillämpats fullt ut i HD, eftersom bara delar av de tidigare uppställda bedömningsgrunderna plockas upp igen.[8]

Att det förefaller finnas viss diskrepans mellan den finmaskiga och komplexa bedömning som HD gav anvisning om i den allmänna delen och den regel som HD sedan verkar ha tillämpat, aktualiserar frågor om vad man som rättstillämpare ska ta med sig från domen.[9] Hur långt räcker egentligen prejudikatvärdet och vad kan vi förvänta oss att domstolarna gör framöver? Jag avser inte att besvara denna fråga i dess fulla teoretiska och praktiska bredd. Orsakerna till det är två: Dels skulle det kräva en väsentligt bredare undersökning än vad som ryms inom ramen för en rättsfallskommentar,[10] dels att man får förvänta sig att det HD sagt har potential till att påverka den faktiska senare rättstillämpningen (särskilt i underinstans och nämnder) alldeles oavsett om det i strikt mening hör till avgörandets ratio decidendi eller inte.[11] Istället kommer jag att fokusera på

med rent pedagogiskt. Avgörandena är numera ofta, om än inte alltid, skrivna så, att mödan först och främst är inriktad på att slå fast en rättsregel, som sedan tillämpas i det konkreta fallet. Inte bara det rättskällematerial som kan vara av betydelse för bestämmandet av rättsregeln redovisas, utan det sker en öppen inventering och värdering av de rättspolitiska argument som kan förtjäna beaktande.”

7 Se Heuman, Metoder för rättstillämpning och lagtolkning (2018) [Heuman (2018)] s. 88 om olika typer av generaliseringar som kan göras för att undvika kasuistisk rättstillämpning och lagtolkning.

8 Sådan diskrepans kan, vilket Heuman (2018) s. 88 påpekar, försvåra prejudikattolkningen.

9 Se närmare om olika metoder för fastställandet av ratio decidendi i ett avgörande, Ramberg, Prejudikat (2017) [Ramberg (2017)], s. 173 ff. och om olika sorters obiter dicta på s. 281 ff. I grunden håller jag också med Heuman när han i sin artikel Ränta på ränta och obiter dicta i JT 1993–94 s. 806 på s. 807 framhåller att det kan vara värdefullt för andra rättstillämpare att HD formulerar sina rättssatser i allmänna termer, men det kan också leda till att onödigt generella rättsregler formuleras vilket åter kan leda till att rättstillämpningen i underinstanser och nämnder inte blir så enhetlig som vore önskvärt.

10 Se exempelvis Helgöstam som i sitt examensarbete Avtalstolkningsprejudikat (Uppsala universitet, höstterminen 2021) gör en sådan analys med fokus på HD-praxis om tolkning av försäkrings- och entreprenadavtal.

11 Se Ramberg (2017) s. 287 om att även obiter dicta i en ”prognos-bemärkelse” kan få högt prejudikatvärde i praktiken. Heuman framhåller att begreppet ratio decidendi inte utgör ett användbart verktyg för att fastställa innebörden av en generell rättsgrundsats när begreppet

att analysera hur HD säger att man ska göra, och vad domstolen faktiskt gör. Det är min förhoppning att detta tillvägagångssätt ska ge läsaren förutsättningar att själv kunna förhålla sig till avgörandet och vad som tycks följa av det.

Förutom formuleringen av mer detaljerade bedömningsgrunder är bedömningen av de konkreta omständigheterna i avgörandet av stort intresse. Genom sin konkreta bedömning visade HD, helt oaktat hur denna förhåller sig till det sätt som HD formulerat i den allmänna delen, att tröskeln för ett obegränsat ansvar enligt 5 a kap. 3 § betaltjänstlagen ska formuleras annorlunda och vara betydligt högre än vad den ofta satts till i underinstansavgöranden de senaste åren. Att HD kom fram till att kundens beteende inte var tillräckligt graverande för att kvalificeras som särskilt klandervärt kan väntas få stor betydelse både för vägledningen av rättstillämpningen framgent och för konsumenternas möjligheter att göra sin rätt gällande. Det finns därför anledning att senare i denna text återkomma i detalj till omständigheterna i målet.

I det följande kommer HD:s dom att analyseras närmare enligt följande huvudrubriker. Först riktas fokus mot HD:s utläggning av rättsregeln och hur domstolen utvecklar mer detaljerade bedömningsgrunder för att kunna avgöra huruvida en konsuments agerande varit ”särskilt klandervärt”. Därefter analyseras omständigheterna i målet i syfte att försöka identifiera vad som mer konkret kan förväntas av en konsument. Sedan kommer ett avsnitt där dels det aktuella avgörandets bäring på fall där bedragaren haft ett annat tillvägagångssätt än i det aktuella målet, dels betydelsen av att de obehöriga transaktionerna genomförts med ett betalningsinstrument som skapats av just bedragaren behandlas. Till sist kommer några avslutande kommentarer.

2. HD:s utveckling av bedömningsgrunder och bedömningen i fallet

HD började i domskälen med att redogöra allmänt för ansvaret för obehöriga transaktioner och regleringen i 5 a kap. betaltjänstlagen, samt de intressen som regleringen ska tillgodose.[12] När HD sedan gick över till att beskriva konto-

används för att beteckna vad som varit avgörande vid bedömningen av det enskilda fallet. Istället bör bedömningen av den generella rättsgrundsatsens kvalitet enligt honom vara inriktad på de generellt verkande domskälen för rättsgrundsatsen och inte på de kasuistiska domskälen som motiverar domslutet i det enskilda fallet. Se Heuman, Kan prejudikatvärdet förbättras? I JT 2021–22 s. 803 på s. 806. Också i Heuman (2018) framhålls på s. 104 att bedömningen av det konkreta fallet inte bör inskränka den beslutade generella rättsgrundsatsens prejudikatverkan, fastän diskrepanser mellan avgörandets generella och specifika delar, vilket han påpekar på s. 88, kan försvåra tolkningen.

[12] Se domskälen p. 8–16.

havarens ansvar vid särskilt klandervärt agerande,[13] gjordes detta genom att HD först visade hur den svenska regleringen i 5 a kap. 2 och 3 §§ betaltjänstlagen förhåller sig till artikel 74 i det andra betaltjänstdirektivet,[14] som regleringen bygger på. Direktivet kräver att kunden ska bära hela förlusten om den har handlat bedrägligt eller avsiktligen underlåtit att uppfylla sina skyldigheter, men att ansvaret utöver dessa fall *får* begränsas i nationell rätt. Den reglering som Sverige på denna punkt valt att anta, innebär i korthet att kunden vid ett grovt oaktsamt åsidosättande av de skyldigheter som åvilar personen enligt 5 kap. 6 § betaltjänstlagen att skydda sitt betalningsinstrument ska ansvara för endast 12 000 kronor om kunden är en konsument, och att det först är vid ett *särskilt klandervärt* agerande som konsumentens ansvar blir obegränsat.

I denna del lyfte HD att också Norge och Danmark har begränsat konsumentens ansvar vid grovt vårdslöst agerande, och våra grannländers reglering av när ett obegränsat ansvar inträffar beskrivs närmare.[15] Den norska och den danska regleringen är inte identisk, men har bland annat det gemensamma draget att lagtexten genom en tydlig regelstruktur med flera rekvisit ger mer konkret vägledning än den svenska, som bara anger att ett till beloppet obegränsat ansvar inträffar om konsumenten har handlat *särskilt klandervärt*.[16]

När HD sedan i p. 22 gick över till att besvara frågan om vilka ageranden som ska anses vara särskilt klandervärda, började domstolen med att beskriva vad som avses med ett grovt vårdslöst agerande enligt regleringen. HD angav i detta sammanhang att det kan vara naturligt att söka ledning i bestämmelser i civilrättslig lagstiftning där samma begrepp används, dock utan att redovisa några sådana. Istället anförde HD med hänvisning till *Mariefreds skola* NJA 1992 s. 130 att begreppet *grov vårdslöshet* inte kan ges en enhetlig innebörd på alla områden där det används och gick vidare till de källor som rör regleringen i betaltjänstlagen. Från skälen till det andra betaltjänstdirektivet lyfte HD att det bör handla om ”ett uppträdande som uppvisar en betydande grad av oaktsamhet”.[17]

[13] Se domskälen p. 17–19.

[14] Europaparlamentets och rådets direktiv (EU) 2015/2366 (PSD2).

[15] Se domskälen p. 20.

[16] Enligt den norska regleringen (lov 2020-12-18-146 om finansavtaler § 4–30 (4)) gäller ett obegränsat ansvar för förluster när kunden uppsåtligen brutit mot sina plikter på ett sådant sätt att kontohavaren måste ha förstått att överträdelsen kunde innebära en närliggande fara för att betalningsinstrumentet skulle missbrukas. Enligt den danska regleringen (lov nr. 652 af 08/06/2017 om betalinger § 100 stk. 5) gäller ett obegränsat ansvar när kontohavaren uppsåtligen lämnat sina personliga behörighetsuppgifter till den som företagit den obehöriga transaktionen under sådana omständigheter att kontohavaren insåg eller borde ha insett att det fanns en risk för missbruk. Det är inte därmed sagt att rättsläget är mycket tydligare i våra grannländer än hos oss, och norska Høyesterett behandlade 23 och 24 augusti 2022 ett mål (22-025299SIV-HRET) som gäller tröskeln för obegränsat ansvar enligt den norska regleringen.

[17] Se domskälen p. 23. Exemplet är hämtat från skäl 72 till det andra betaltjänstdirektivet.

När HD i p. 24 gick in på de svenska förarbetsuttalandena om tröskeln för grov oaktsamhet, återgavs formuleringen att det ”måste vara fråga om ett markant avsteg från aktsamhetsnormen där kontohavaren har varit obetänksam i en sådan grad att han eller hon inte är ursäktad; lindriga fall av slarv eller tillfällig glömska utgör därför inte ett grovt oaktsamt agerande”.[18] Formuleringen är tvetydig och kan ha bidragit till att skapa osäkerhet om ansvarsbedömningen och att praxis från ARN och underinstanserna ofta blivit sträng mot konsumenten och tidvis något spretig.[19] Början av meningen, att det ”måste vara fråga om ett markant avsteg från aktsamhetsnormen” tyder visserligen på en grövre vårdslöshet, medan övriga delar – ursäktlig obetänksamhet, lindriga fall av slarv eller glömska – istället påminner om hur man kunde beskriva den nedre gränsen för ett vanligt culpaansvar, inte den övre.[20]

HD återgav i denna punkt bara vad som framgår av förarbetena, men man kan fundera över att HD gör så utan att närmare kommentera meningen. Genom den närmare beskrivningen av tröskeln för särskilt klandervärt agerande i nästa punkt (p. 25) får man emellertid en inblick i vad HD menade. HD valde nämligen att lyfta bara den första delen av den citerade meningen och framhöll att det, för att agerandet ska anses ”särskilt klandervärt, krävs något *mer än* ett agerande som är grovt vårdslöst” och att agerandet alltså ska vara ”*allvarligare än* ett *markant avsteg* från normal aktsamhet” (mina kursiveringar). Exemplifieringen i förarbetena utgör alltså tveklöst exempel på situationer som inte når upp till tröskeln ”särskilt klandervärt” agerande, men det är nu, efter HD:s ställningstagande, än mer tydligt att de heller *inte* kan läsas eller uppfattas som exempel som ligger *nära* tröskeln.

[18] HD citerade här prop. 2009/10:122 s. 27 ff.

[19] ARN har med något undantag gjort bedömningen att det varit särskilt klandervärt att lämna ut 3–6 svarskoder till någon annan (ARN 2013-04700, 2017-10285 I och II och 2019-19154), medan att legitimera sig med BankID gentemot den bank som bedragaren utgivit sig för att ringa från och då det saknats utredning om vilken text som eventuellt kommit upp i BankID:et då beställning av nytt BankID gjorts, bedömts vara grovt oaktsamt (ARN 2017-07814 och 2017-13660). Att lämna ut svarskoder från bankdosan är visserligen ett tydligt åsidosättande av de skyldigheter som åligger kunden, men inte i mer än ett av de fall som redovisats som vägledande i ARN eller underinstans finns hållpunkter som ens antyder att det handlar om en *likgiltighet* eller något som kan påminna om ett *medvetet* risktagande från kundens sida. ARN 2017-10285 II innehåller en relativt kortfattad beskrivning av ARN:s bedömning, men i detta referat finns åtminstone en viss antydan om att kunden kanske inte hållit sig helt till sanningen i samband med utredningen av bedrägeriet.

[20] De konkreta exemplen som ges i förarbetena ansågs av HD ge begränsad ledning eftersom de gäller kontokort, och inte andra betalningsinstrument. Det är lätt att vara enig med HD om att det finns betydande skillnader mellan olika betalningsinstrument, men *varför* HD ansåg att uttalandena är så ointressanta får man som läsare ingen insyn i. En orsak kan vara att det inte har varit vanligt förekommande att en kontoinnehavare genom personlig kontakt med en bedragare lurats att ge ifrån sig vare sig behörighetsfunktioner eller själva kontokortet och att situationerna därför inte är särskilt jämförbara.

Därefter lyftes att det särskilt är fall där handlandet utgör ”en kvalificerad form av grov oaktsamhet som avses” och att ”regleringen ska träffa fall där konsumenten har agerat så klandervärt i förhållande till betaltjänstleverantören att det skulle vara stötande att leverantören behövde stå för någon del av beloppet”. HD ansåg att det enligt förarbetena därför rör sig om fall där ”konsumenten genom sitt handlande får anses ha varit likgiltig till risken för obehöriga transaktioner”.[21]

Mot bakgrund av den ovan beskrivna genomgången av rättskällorna angav HD sedan i p. 26 och 27 tre situationer när konsumenten ska ansvara för hela beloppet som förts över med en obehörig transaktion. Den första följer direkt av direktivet, nämligen om konsumenten har agerat bedrägligt. Enligt HD bör detsamma gälla när ”konsumenten *med avsikt* har överlämnat personliga behörighetsfunktioner, t.ex. inloggningsuppgifter till BankID eller koder till en bankdosa, *till en obehörig person* och då *insåg eller hade anledning att misstänka* att det förelåg en *betydande eller närliggande risk* för att hans eller hennes handlande kunde medföra en förlust” (mina kursiveringar). Det framgår inte i denna punkt uttryckligen om HD anser att konsumentens avsikt att överlämna de personliga behörighetsfunktionerna måste täcka bara själva överlämnandet (att man medvetet ger ifrån sig behörighetsfunktionen till någon), eller om avsikten även måste inrymma att detta sker till en obehörig person (insikt om att personen är obehörig). Denna otydlighet undanröjs när HD senare, under bedömningen i det konkreta fallet, angav att det inte var bevisat att konsumenten ”avsiktligen lämnade ut koderna till en obehörig person”.[22] Att kunden i målet hade varit medveten om att han lämnade ut en svarskod från bankdosan och att det objektivt sett skedde till en obehörig person, är trots allt tydligt.

Det andra typfallet av *särskilt klandervärt handlande* som HD uppställde, är när ”konsumenten – även om han eller hon inte avsiktligen överlämnade en personlig behörighetsfunktion till någon obehörig – var likgiltig till risken för obehöriga transaktioner”. HD angav därefter att ett särskilt klandervärt agerade ”alltså” föreligger när konsumenten ”var medveten om, dvs. faktiskt insåg, att det fanns en risk för en obehörig transaktion men ändå agerade på ett sätt som innebar ett brott mot 5 kap. 6 §”. Det är alltså först då konsumenten haft faktisk insikt om risken för obehöriga transaktioner som det är närliggande att anse att kunden varit *likgiltig* inför denna risk.

Vid första anblick kan det vara oklart om detta förtydligande och kravet om faktisk insikt gäller bägge de av HD uppställda typfallen, eller bara det sista. Det senare torde emellertid vara den riktiga tolkningen. Det första typfallet kombinerar trots allt redan i sig ett krav om avsikt avseende överlämnande av personliga behörighetsfunktioner till obehörig person och en bedömning av om kunden ”insåg eller hade anledning att misstänka” att det förelåg en ”betydande

[21] Domskälen p. 25 och prop. 2009/10:122 s. 17 f. och 27 ff.
[22] Se domskälen p. 34.

eller närliggande” risk för förlust. Ett ”förtydligande” om faktisk insikt avseende risken för en obehörig transaktion skulle då leda till ett åsidosättande av delar av en nyss angiven bedömningsgrund.

Det sätt på vilket HD formulerade de två bedömningsgrunderna, kan förväntas få särskilt stor betydelse för ansvarsbedömningarna i de fall då kunden utsatts för ett bedrägeri. HD framhöll också att det vid bedömningen av vad konsumenten faktiskt insett får särskild betydelse *till vem* konsumenten uppfattat att den personliga behörighetsfunktionen lämnats ut. Fastän HD i p. 27 angav att ett obegränsat ansvar förutsätter faktisk insikt hos konsumenten, framhöll domstolen i p. 28 att bedömningen av om konsumenten har agerat särskilt klandervärt ”i princip” ska göras ”objektiverat”. Med detta menade HD att bedömningen ska göras utifrån ”hur en konsument [i] av *motsvarande slag* [ii] i *samma situation* [iii] *typiskt sett* skulle ha agerat” (mina kursiveringar och numreringar). HD angav också några faktorer som det i detta sammanhang finns anledning att fästa särskilt avseende vid, nämligen den miljö och situation som konsumenten befann sig i, konsumentens ålder och erfarenhet, och hur förslaget bedrägeriet har varit.

I samband med bedrägeriets förslagenhet angav HD även en ytterligare faktor som vid första anblick kan uppfattas svårförenligt med det krav om faktisk insikt om risken för obehöriga transaktioner som HD nyss uppställt, nämligen ”vad konsumenten förstått eller borde ha förstått beträffande de uppgifter som lämnades till bedragaren och de möjliga konsekvenserna av att de lämnades ut”. Här får man nog förstå HD som att det inte handlar om att låta ansvarsbedömningen som sådan bero på vad konsumenten borde ha förstått, men istället det något självklara: att graden av kunskap, förståelse och vårdslöshet gällande att personen utsatts för ett bedrägeri givetvis kommer vara av betydelse för de bedömningar som ska göras enligt de bedömningsgrunder som HD uppställt.[23] Samtidigt är det svårt att se hur man ska förena ett krav om faktisk insikt med en bedömning av vad kunden borde ha förstått.[24]

Vad HD egentligen har menat på denna punkt och hur de olika faktorerna ska förstås i relation till de två typfallen av särskilt klandervärt beteende som beskrivs, och i relation till kravet om faktisk insikt om missbruksrisken som HD själv formulerat, är helt enkelt lite oklart. Det blir nämligen inte alldeles lätt att veta hur bedömningen bör struktureras eller hur de olika rekvisitliknande formuleringarna förhåller sig till varandra, när flera bedömningsgrunder

[23] Man kan notera att det är uppgifterna som lämnades till bedragaren och de möjliga konsekvenserna därav som HD nämnde, inte hur konsumenten borde ha uppfattat uppgifterna som lämnades av bedragaren. Samtidigt är det svårt att bortse ifrån att uppgifterna som lämnats av bedragaren kan påverka kundens bedömning av de potentiella konsekvenserna av att lämna ut sina behörighetsfunktioner.

[24] För den otåliga läsaren kan redan här avslöjas att HD inte uttryckligen hanterade detta i sin konkreta bedömning.

ständigt presenteras utan att deras inbördes relation till varandra uttryckligen kommenteras.

Sådan oklarhet kan leda till att avgörandets funktion som vägledning för rättstillämpningen försvagas och att avgörandet i mindre utsträckning än vad som vore önskvärt leder till enhetliga och förutsebara bedömningar.[25] Viss risk finns även att underinstanser och andra i sin tolkning av avgörandet förleds att även fortsättningsvis luta mot en mer eller mindre traditionell culpabedömning. När det gäller bedömningen av det aktuella fallet från och med p. 30 bör man emellertid notera att HD nästan uteslutande fokuserade på att beskriva hur kunden faktiskt uppfattat situationen, inte på att problematisera huruvida dessa uppfattningar varit rimliga eller befogade. Det är därför tydligt att HD inte själv avgjorde målet efter en klassisk culpabedömning. Genom bedömningen i det konkreta fallet, får man alltså även på denna punkt viss ledning om hur HD:s tidigare domskäl bör förstås.

Man kan dock fundera över att HD drog slutsatsen att kunden inte agerat särskilt klandervärt utan att överhuvudtaget anknyta till några av de faktorer som domstolen i p. 28 uppställt för hur den påstått objektiverade bedömningen ska gå till. HD anknöt alltså i sin konkreta bedömning inte alls till hur en konsument av motsvarande slag i samma situation typiskt sett skulle ha agerat, utan verkar bara ha fokuserat på hur just denna konsument uppfattat saker. HD fastslog också att det av utredningen framgått att kunden blev utsatt för ett förslaget bedrägeri, dock utan att göra någon bedömning av vad kunden *borde ha förstått* beträffande de uppgifter som lämnats till bedragaren och de möjliga konsekvenserna av att de lämnats ut.

I den konkreta bedömningen tog HD egentligen inte heller utgångspunkt i någon av de av HD själv formulerade bedömningsgrunderna, men när HD i p. 34 summerade sin bedömning, får man reda på vilka grunder som konkret bedömts. Här konstaterade HD först att det inte bevisats att kunden avsiktligen lämnat ut koderna till en obehörig person. HD gick därför inte, som jag uppfattar det, vidare till någon bedömning av de övriga rekvisiten i denna bedömningsgrund, nämligen huruvida kunden hade haft insikt om eller hade haft anledning att misstänka, att det förelåg en betydande eller närliggande risk för förlust. Samtidigt överlappar åtminstone delar av denna bedömningsgrund med den andra bedömningsgrunden som HD uppställt, vilken enligt HD inte heller ledde till ett obegränsat ansvar eftersom det inte bevisats att kunden hade ”insikt om att det fanns en risk för de obehöriga transaktioner som kom att utföras” och att det därför ”inte varit fråga om ett sådant agerande som krävs för att en konsument ska anses ha handlat särskilt klandervärt”.

[25] Se om ett avgörandes vägledningskapacitet som kvalitetskriterium Heuman, JT 2021–22 s. 803 på s. 807.

3. Närmare om omständigheterna i målet och HD:s bedömning av dessa

HD kom alltså fram till att kunden inte hade agerat särskilt klandervärt eftersom det inte hade bevisats att kunden avsiktligen hade lämnat ut sina koder till en obehörig person och att det heller inte hade bevisats att kunden haft insikt om risken för de obehöriga transaktionerna som möjliggjordes genom hans agerande. Som nämnts ovan, verkar det som att HD:s konkreta bedömning uteslutande bygger på hur den aktuella konsumenten rent faktiskt uppfattat situationen, samtidigt som domstolen själv tidigare i domskälen beskrivit att bedömningen av om kunden agerat särskilt klandervärt ska ske objektiverat mot bakgrund av hur en konsument av motsvarande slag i samma situation typiskt sett skulle ha agerat.

Detta behöver inte betyda att sådana överväganden inte lagts till grund för HD:s slutsats. Ska man i sin tolkning av avgörandet utgå ifrån att HD också själv gjort som domstolen sagt att man ska göra, får man kanske utgå från att kunden i det aktuella målet agerat som ”jämförelsekonsumenten” skulle ha gjort. Huruvida man kan, får eller bör göra ett sådant antagande, kan det emellertid råda olika uppfattningar om. Oavsett kan bristen på närmare diskussion och problematisering av de olika omständigheterna i målet föranleda en närmare analys, för att på så vis försöka identifiera vad som egentligen kan förväntas av en konsument.

Konsumenten hade en torsdagseftermiddag i augusti 2018 blivit uppringd av en person som uppgav sig ringa från säkerhetsavdelningen på en av de två banker hos vilka konsumenten var kund, men i själva verket var det en bedragare som ringde. Personens ärende angavs vara att inhämta kundens samtycke till fortsatt lagring av persondata enligt den då nya dataskyddsförordningen (GDPR). När HD gick över i bedömningen av det konkreta fallet, började domstolen med att beskriva en mer allmän omständighet kopplad till detta som kunde underbygga att kundens uppfattning kunde ha fog för sig. HD konstaterade här att dataskyddsförordningen i betydande omfattning hade aktualiserat kontakter mellan företag och konsumenter. Det sades inte rakt ut, men att anledningen till samtalet som bedragaren gett hade framstått som rimlig för kunden, verkar ha varit en central omständighet för HD:s bedömning, och det är mot denna bakgrund som övriga delar av kommunikationen mellan kunden och bedragaren analyseras. Att det ärende bedragaren uppger sig ha i sak måste framstå som rimligt och förnuftigt för att kunden ska kunna lämna ut personliga behörighetsfunktioner utan att riskera ansvar för följande obehöriga transaktioner, framstår som rätt uppenbart. Detta kan dock inte utgöra mer än en utgångspunkt för bedömningen.

Bedragaren hade vidare uppgett att kunden inte hade besvarat ett brev där banken krävt skriftligt samtycke, och att kunden senast nästföljande dag var tvungen att gå till ett bankkontor och godkänna bankens personuppgiftshante-

ring för att inte bli struken som kund i banken. Kunden, vilken hade befunnit sig på sitt arbete och därför inte haft möjlighet att gå till bankens kontor, hade då frågat om det gick att lämna sitt godkännande via e-post, vilket bedragaren sade att banken av säkerhetsskäl inte kunde godta. HD gjorde i p. 31 bedömningen att kunden fått uppfattningen att det krävdes brådskande åtgärder från kundens sida för att han inte skulle förlora möjligheten att använda sitt konto och att kunden hade blivit stressad av detta. HD sade emellertid inget om huruvida det var rimligt av konsumenten att tro att banken verkligen skulle ha kontaktat honom så nära inpå en avgörande frist att han i realiteten skulle behöva dyka upp på ett bankkontor redan samma eller nästföljande dag. Det kan också diskuteras om det var rimligt att tro på att banken, efter bara *ett brev* och *ett samtal* dagen före sista frist, skulle vara beredd att vidta en så allvarlig åtgärd som att spärra kontot. Inte heller kommenterade HD huruvida kunden rent faktiskt fått ett sådant brev från banken, såsom bedragaren hävdade.

Kunden hade därefter frågat om det inte fanns något annat sätt att ge sitt godkännande, varpå bedragaren uppmanade kunden att logga in i internetbanken med sitt BankID. Den text kunden fick upp i sitt BankID angav emellertid att det kunden gjorde, var att legitimera sig gentemot en annan bank än den från vilken personen uppgav sig ringa. Kunden ifrågasatte detta, men lugnades av bedragarens förklaring att orsaken var att själva BankID:et hade utställts av den andra banken. HD ansåg (p. 32) att det framgick av utredningen att kunden hade uppfattat bedragaren som en ”lugn och seriös banktjänsteman som gav förklaringar som [kunden] uppfattade som rimliga till de frågor han ställde” och (p. 33) att bedragaren under det första samtalet lyckats skapa ett förtroende hos kunden och förmått kunden att själv föreslå de lösningar som gav bedragaren möjlighet att vid det andra samtalet skapa ett nytt BankID och genomföra de obehöriga transaktionerna. HD sade emellertid inget om att den förklaring bedragaren gett till varför fel banks namn dök upp i BankID:et, innehöll ett sakfel som kunden åtminstone rent objektivt haft förutsättningar för att avslöja. Enligt uppgifter som framgår av bankens utveckling av sin talan i tingsrättens referat framgår nämligen att BankID:et inte var utställt av den andra banken, utan av den bank som bedragaren uppgav sig ringa ifrån.[26]

Efter att kunden hade godkänt villkoren för personuppgiftshantering påstod bedragaren att kundens BankID var gammalt och behövde förnyas, vilket sades skulle behöva göras på ett av bankens kontor. Även denna gång frågade kunden om det inte fanns alternativ till ett platsbesök, varpå bedragaren berättade att det i så fall skulle kräva att kunden använde sin bankdosa. Eftersom kunden inte haft denna med sig på arbetet kom de överens om att talas vid senare samma

[26] Se Stockholms tingsrätts dom i mål T 17521-19 s. 7, sista stycket första meningen och s. 8 första stycket sista meningen. Inte heller skulle förklaringen, om nu BankID:et var utställt av den andra banken, vara objektivt sett korrekt. Att vanliga konsumenter inte kan förväntas ha koll på den sortens tekniska detaljer är emellertid rätt uppenbart.

kväll. Dessa omständigheter, eller huruvida det var rimligt att en banktjänsteman från en bank skulle ha insyn i att ett BankID utställt från en annan bank behövde förnyas och att det skulle vara något som banktjänstemannen skulle kunna hjälpa till med, kommenteras inte uttryckligen av HD utöver det som tidigare återgetts om att bedragaren gett vad kunden uppfattat som rimliga förklaringar. Vid det andra samtalet hade kunden följt bedragarens instruktioner, tryckt in siffror i bankdosan och lämnat ut svarskoder från bankdosan, vilket alltså gjort det möjligt för bedragaren att beställa ett nytt BankID i kundens namn vilket sedan användes för att föra över pengar från kundens konto.

Det finns alltså en del saker att reagera på i de uppgifter bedragaren hade lämnat till kunden, och det är inte svårt att hitta felaktigheter eller andra konstigheter som *kunde* ha fått kunden att reagera. Vad en normal konsument kan förväntas reagera på måste emellertid bero på om det krävs särskild erfarenhet och teknisk- eller juridisk kompetens för att avslöja att uppgifterna inte stämmer. Handlar det om faktaupplysningar som kunden kunde ha avslöjat som oriktiga utan någon särskild kompetens, kan det finnas anledning att ställa högre krav på konsumenten.

Mot denna bakgrund är det lite besvärande att HD inte kommenterade huruvida det är rimligt att inte ha koll på vilken bank som utställt ens BankID eller vilken post man fått från banken. Dessa uppgifter måste också ha varit viktiga för bedömningen av övriga uppgifter bedragaren lämnade. Uppgiften om från vilken bank BankID:et hade utställts av var helt avgörande för att bedragarens förklaring till varför den andra bankens namn dök upp skulle kunna bedömas som trovärdig. Uppgiften om bankens tidigare försök att inhämta samtycke från kunden torde ha gjort att det verkade mer rimligt att uppringningen skedde så sent att det nu verkligen brådskade. Övriga felaktigheter och konstigheter i de uppgifter bedragaren hade lämnat är det enligt min mening mindre problematiskt att HD underlät att diskutera. Orsaken är att ett avslöjande av dessa som felaktiga torde förutsätta betydligt större inblick i och förståelse av hur BankID fungerar än vad en normal konsument kan förväntas ha.

När jag ovan har försökt peka på saker som inte riktigt hänger ihop i bedragarens förklaring och som konsumenten åtminstone kunde ha reagerat på, får det inte uppfattas som ett uttryck för att jag anser att HD hamnat fel i sin slutsats att konsumentens agerande ”bara” var grovt oaktsamt. Tvärt om anser jag att HD hamnade i en förväntad och korrekt slutsats. Syftet är snarare att visa att det kan finnas rätt många saker som brister i en bedragares förklaringar, utan att det behöver leda till att konsumenten ska anses ha agerat särskilt klandervärt. Och just det är något som kan förväntas få mycket stor betydelse för hur denna typ av mål bedöms framöver.

4. Närmare om (den bristande) betydelsen av bedragarens tillvägagångssätt och prejudikatets räckvidd

En av utmaningarna med att konkretisera ansvarsbedömningen vid obehöriga transaktioner är att det sätt på vilket denna sorts bedrägerier genomförs varierar, och ständigt ändras. Detsamma gäller hur olika betalningsinstrument fungerar och hur säkerhetsanordningarna som syftar till att reducera risken för obehörig användning utformats.[27]

Ett exempel på variationer kopplat till det sista är vilken sorts information som dyker upp i BankID:et vid olika dispositioner. Förutom att BankID som verktyg ständigt utvecklas och ändras,[28] har betaltjänstleverantörerna ofta viss valfrihet med hänsyn till vilken information de vill ska dyka upp när BankID:et används till *annat än* att godkänna en betalning, något som kan göra det svårare för kunden att veta vad den kan förvänta sig och vad som är normalt.[29] Ett annat exempel är om det BankID som används måste befinna sig på samma fysiska ställe som den enhet där dispositionen företas eller inte.[30] Ett tredje exempel är om det krävs en kombination av användning av BankID och en traditionell bankdosa för att genomföra vissa dispositioner. I flera banker kan man beställa ytterligare mobila BankID uteslutande med hjälp av sitt befintliga mobila BankID, men i det aktuella målet verkar koddosan ha behövts, eller åtminstone föredragits av bedragaren.

HD har i avgörandet haft fokus på situationen då konsumenten har *överlämnat personliga behörighetsfunktioner* till en person som visar sig vara obehörig. HD framhöll också att kunden uppvisat en betydande vårdslöshet ”genom att vid det andra samtalet lämna ut koderna från bankdosan”.[31] Detta kan ge intryck av att det bara är just utlämnandet av koder som var grovt vårdslöst och inget annat. Eftersom konsumenten hade lämnat ut svarskoder från sin bankdosa och även erkänt att han agerat grovt oaktsamt, är det givetvis rimligt att

[27] Stora variationer och ständiga ändringar gör det också mycket svårt för även intresserade och försiktiga konsumenter att hålla koll på vad som är normalt och inte.

[28] Exempelvis verkar det ha varit först i februari 2022 som möjligheten öppnades för att myndigheter och företag skulle kunna lägga in information om avsikten med en identifiering i BankID, se https://www.bankid.com/om-oss/nyheter/text-om-avsikt-hoejer-saekerheten-vid-identifiering (läst 8 augusti 2022).

[29] Vid godkännande av elektroniska betalningstransaktioner på distans gäller däremot krav om att använda stark kundautentisering som kopplar transaktionen till ett specifikt belopp och en specifik betalningsmottagare, se 5 b kap. 4 § andra stycket betaltjänstlagen.

[30] För några få år sedan infördes möjligheten för skanning av QR-kod som extra säkerhetsfunktion när det BankID som används finns på en annan digital enhet än den på vilken en inloggning, transaktion eller annat företas. Det finns emellertid sätt att kringgå även sådana funktioner, exempelvis genom att bedragaren skickar en bild på den QR-kod som dyker upp på hans eller hennes dator, samtidigt som kunden får besked att skanna denna bild med sin mobiltelefons kamera.

[31] Se domskälen p. 34.

frågan inte diskuteras närmare. Dock kan detta fokus på just överlämnande av personliga behörighetsfunktioner innebära att osäkerhet uppkommer gällande avgörandets betydelse för framtida rättstillämpning i fall där konsumenten *inte* givit ut personliga behörighetsfunktioner men ändå, efter att ha utsatts för ett förslaget bedrägeri, rent faktiskt har bidragit till att obehöriga transaktioner kunnat genomföras.

Detta kan typiskt sett ske på två sätt. *Det ena* är om kunden själv har godkänt transaktionen med sitt BankID, om än efter att ha blivit vilseledd av bedragaren. I dessa fall är emellertid transaktionen att anse som *behörig*, varför frågan om ansvarsfördelning mellan kund och bank inte uppkommer.[32] *Det andra* är om transaktionen godkänts med ett betalningsinstrument som utställts i kundens namn, men som kunden inte vet om att det existerar, eftersom det beställts och kontrolleras av bedragaren.[33] I dagens digitala verklighet är det alltså inte nog att kunden noga skyddar de betalningsinstrument och personliga behörighetsfunktioner som den själv har fått från banken. För att vara säker, måste också förhindras att någon annan får möjlighet att själv skapa *nya* betalningsinstrument i kundens namn, vilket alltså ofta har skett genom att kunden har lurats att godkänna sådana beställningar med sitt befintliga BankID, utan att själv förstå att det är vad som händer.[34]

Detta anknyter till en problematik som HD inte uttryckligen hanterar i mål T4623-21, nämligen betydelsen av att kundens brister inte nödvändigtvis rört hanteringen av BankID:et eller bankdosan *som betalningsinstrument*, utan som *legitimeringsverktyg och som elektronisk underskrift* i samband med beställning av ett nytt BankID, vilket sedan använts för att genomföra de obehöriga

[32] En transaktion är enligt 1 kap. 4 § första stycket moment 34 betaltjänstlagen obehörig om den genomförs *utan samtycke* från kontohavaren eller någon annan som enligt kontoavtalet är behörig att använda kontot. Frågan om transaktionen varit obehörig ska avgöras enligt vad som fastställdes i NJA 2017 s. 1105. Betaltjänstleverantören har bevisbördan för att en transaktion har genomförts med kontohavarens betalningsinstrument, medan kontohavaren sedan har att göra *antagligt* att det inte är innehavaren själv, eller någon med dennes samtycke, som genomfört transaktionen. Är det innehavaren av BankID:et själv som har godkänt transaktionen är den alltså att anse som behörig, och det gäller även i de ofta förekommande fallen då innehavaren utsatts för bedrägeri och lurats godkänna transaktionen. Se t.ex. ARN 2019-11253, ARN 2019-14354 och ARN 2019-08258. Förutsättningen för att transaktionen ska anses behörig är emellertid att den information som framgått i BankID:et uppfyller kraven i 5 b kap. 4 § andra stycket betaltjänstlagen så att det tydligt framgår att det som godkänts varit en betalning med visst belopp till viss mottagare.

[33] Den senare situationen har likhetsdrag med vad som hände i HD:s mål *BankID-bedrägeriet* förutom att kunden där var medveten om att ett nytt BankID beställdes, även om han hade vilseletts till att tro att det handlade om att uppdatera det BankID han själv använde.

[34] Viss kritik har, med rätta, riktats mot att det, när bedragaren först släppts in i kundens internetbank, är nära på ”fritt fram” för att både skapa nytt Mobilt BankID och genomföra transaktioner som uppenbart inte motsvarar kundens normala användningsmönster. Se https://www.dagensjuridik.se/nyheter/det-talar-att-bankerna-ska-sta-pengar-som-forsvinner-vid-bedragerier-skarp-sakerheten/ (besökt 8 augusti 2022).

transaktionerna.[35] Legaldefinitionen av ett betalningsinstrument är enligt 1 kap. 4 § första stycket moment 9 betaltjänstlagen ”ett kontokort eller något annat personligt instrument eller rutin som enligt avtal används för att initiera en betalningsorder”. När ett BankID används till *annat än* att initiera en betalningsorder, används det alltså inte som ett *betalningsinstrument* och är därför inte föremål för reglering i 5 och 5 a kap. betaltjänstlagen.[36]

Bankens ansvar för att återställa kontot enligt 5 a kap. 1 § betaltjänstlagen är oberoende av om den obehöriga transaktionen genomförts av annan med hjälp av kundens betalningsinstrument, ett betalningsinstrument som getts ut till bedragaren i kundens namn, genom digital manipulation eller på annat vis. I alla dessa fall handlar det om obehöriga transaktioner på kundens konto. Bestämmelsen i 5 a kap. 3 § jämförd med 5 kap. 6 § uppställer emellertid endast ansvar för kunden till följd av dennes brister i att skydda *de personliga behörighetsfunktioner som är knutna till betalningsinstrumentet* och att följa de villkor som gäller för användningen av *betalningsinstrumente*t. Regleringen verkar alltså bygga på en förutsättning att det betalningsinstrument som använts utställts till den aktuella kunden på korrekt vis.[37]

Om de obehöriga transaktionerna genomförts med ett betalningsinstrument som kunden inte själv beställt eller ens varit medveten om att det har utgivits, är det därför något ansträngt att se det som att den obehöriga transaktionen har kunnat genomföras till följd av att kunden har åsidosatt skyldigheterna att skydda *sitt* betalningsinstrument eller de till betalningsinstrumentet knutna personliga behörighetsfunktionerna (som kunden alltså inte känner till).

Det verkar *rimligt* att utgå ifrån att beteendet strider mot användarvillkoren som kunden är bunden av enligt avtal med både banken och utgivaren av BankID:et, om dessa inte är samma aktör. Samtidigt kan det ifrågasättas om villkor som *inte* gäller kundens hantering av BankID eller bankdosa *som betalningsinstrument* ska kunna leda till ett ansvar med stöd i 5 a kap. 3 § jämförd med 5 kap. 6 § första stycket 3 betaltjänstlagen. Dessutom kan det diskuteras om det verkligen är nödvändigt (och ur säkerhetssynpunkt acceptabelt) att beställning av nya betalningsinstrument kan göras så snabbt och enkelt som idag. Det som ur praktisk synvinkel är mycket lyckat, nämligen att ett och samma verktyg med stor lätthet kan användas för olika ändamål och i olika sammanhang, blir i

[35] I det aktuella målet hade svarskoder från bankdosan lämnats ut, och det kan därför sägas ha varit ren slump (för konsumenten) att bedragaren hade valt att använda koderna för att skapa ett nytt BankID istället för att godkänna de aktuella transaktionerna.

[36] Annorlunda är det i den norska regleringen i nya finansavtaleloven (lov-2020-12-18-146) § 3–20 som likställer ansvaret för förlust till följd av obehörig användning av e-legitimation som signatur och som betalningsinstrument.

[37] Som *BankID-bedrägeriet* visar behöver emellertid inte så vara fallet, och i praxis tycks inte vare sig Högsta domstolen, underinstanserna eller ARN göra någon principiell skillnad på kundens ansvar för obehöriga transaktioner beroende på om transaktionerna genomförts med hjälp av kundens eget betalningsinstrument eller med ett betalningsinstrument som beställts av bedragaren och installerats på dennes mobiltelefon.

detta sammanhang en omständighet som kan skapa osäkerhet kring regleringens tillämpning.

Det skulle emellertid givetvis leda till oacceptabla resultat om kunden kunde låta obehöriga personer gå in i internetbanken och medverka till att ett nytt betalningsinstrument utges till bedragaren, utan att riskera att bli ställd till svars för de obehöriga transaktioner som därmed möjliggörs.[38] Särskilt gäller detta eftersom de efterföljande transaktionerna som görs med det nya mobila BankID:et är att anse som obehöriga transaktioner som enligt 5 a kap. 1 § ska återställas och att det bara är tillfälligheter, vanligen bedragarens val av tillvägagångssätt, som avgör om agerandet omedelbart leder till en obehörig transaktion eller inte.

Konsekvensen av en sträng tolkning av 5 a kap. 3 § betaltjänstlagens tillämpningsområde skulle dock inte nödvändigtvis leda till att förlusten slutligt skulle hamna på *betaltjänstleverantören*. Om kunden genom att släppa in obehöriga i internetbanken har möjliggjort för att ett nytt betalningsinstrument har beställts, och därmed har brutit mot villkor i de avtal som gäller med banken eller utställaren av BankID:et, kunde man istället tänka sig att kundens avtalsbrott skulle leda till att kunden åläggs ett kontraktsrättsligt ersättningsansvar för bankens förlust till följd av att den varit skyldig att återställa kundens konto.[39]

En sådan rättstillämpning skulle emellertid innebära ett tydligt åsidosättande av det skydd som följer av 5 a kap. 1 § betaltjänstlagen. Att komplettera regleringen med annars gällande principer för inomkontraktuellt ansvar skulle nämligen leda till ett väsentligt mer långtgående ansvar för kunden i de fall då bedragaren varit förslagen nog att först skaffa sig ett nytt mobilt BankID i kundens namn, istället för att direkt genomföra den obehöriga transaktionen. Att på detta vis *sänka* tröskeln för kundens ansvar i ett typfall som ur kundens perspektiv kan vara än svårare att avslöja som ett bedrägeri, framstår som mindre välmotiverat. Det kan också diskuteras om inte regleringen i 5 a kap. betaltjänstlagen, som trots allt är tänkt att balansera motstående intressen och i icke oväsentlig omfattning utgöra en skyddsreglering för kunderna, bör anses *uttömmande* reglera kundens potentiella ansvar. Att komplettera regleringen med allmänna principer för inomkontraktuellt skadestånd framstår mot denna bakgrund som principiellt problematiskt.[40] Samtidigt skulle det leda till olämpliga resultat att tillämpa ansvarsregeln i 5 a kap. 3 § jämförd med 5 kap. 6 § strikt

[38] Att legitimera sig med sitt BankID på uppmaning av någon annan utan direkt insyn i vad legitimeringen används till, är ett beteende som nog ofta får anses som vårdslöst, och beroende på omständigheterna i övrigt även grovt vårdslöst. Istället för en mer eller mindre typiserad bedömning enligt vilken det så gott som alltid är grovt vårdslöst att lämna ut koder, får ett eventuellt ansvar i dessa fall istället bedömas mot bakgrund av vilken information som dykt upp i kundens BankID. Ju mer detaljerad information, desto större möjlighet för att anse att kunden agerat vårdslöst.

[39] Ansvar förutsätter då att det finns villkor i de avtal kunden slutit med banken och att villkoren och kundens skyldigheter är tillräckligt tydligt formulerade.

[40] Dessutom kan det ifrågasättas om situationen alls är jämförbar med en klassisk avtalssituation till följd av kombinationen begränsad avtalsfrihet (man ”måste” ha BankID), standardavta-

efter ordalagen och principiellt utesluta ansvar för kunden i alla de fall då själva de obehöriga transaktionerna gjorts med ett betalningsinstrument upprättat av bedragaren. Fastän ansvarsbedömningen nödvändigtvis kommer att påverkas av hur bedrägeriet konkret har gått till, framstår det också som en synnerligen dålig och oförutsägbar ordning om kundens ansvar vid obehöriga transaktioner på det egna kontot ska bedömas efter olika mönster beroende på bedragarens tillvägagångssätt i det enskilda fallet.[41]

Fastän slutsatsen inte har så tydligt stöd i vare sig lagstiftningen eller praxis som vore önskvärt, verkar den i sammanhanget klart bästa lösningen vara att tillämpa ansvarsreglerna i 5 a kap. 2–6 §§ betaltjänstlagen också i fall då kundens eventuella vårdslöshet gäller hanteringen av den egna e-legitimation på ett sätt som har möjliggjort skapande av nya betalningsinstrument, som sedan använts för att genomföra obehöriga transaktioner. Efter *BankID-bedrägeriet* får denna slutsats också anses ha visst stöd i praxis, trots att frågan inte uppmärksammades uttryckligen. Detta leder alltså till en i viss omfattning utvidgad tolkning av kundens skyldigheter, genom att plikten att skydda sitt betalningsinstrument också får anses innebära en plikt att förhindra att nya betalningsinstrument ges ut i kundens namn, samtidig som tolkningen innebär ett ökat skydd för kunden jämfört med det annars mest närliggande alternativet.

5. Slutord

Det torde redan ha framgått att jag anser att HD träffat rätt i sin slutsats, när den gjort bedömningen att den aktuella konsumentens agerande inte var att anse som särskilt klandervärt. Avgörandet innebär enligt min uppfattning också ett viktigt steg i riktning mot att realisera det konsumentskydd som lagstiftaren har förordat i förarbetena, men som för många konsumenter hittills har visat sig svårt att uppnå i praktiken. I grunden anser jag också att HD:s operationalisering av rekvisitet ”särskilt klandervärt” är lyckad, och på ett fint sätt balanserar hänsynen mellan konsument och kontoförande bank. Därtill får man väl tillåta sig att, som nordist, uppskatta HD:s utblickar till övrig nordisk rätt och att domstolen så tydligt verkar ta ledning av hur våra grannländer utformat sina regler på området.

Samtidigt är det något olyckligt att HD inte genom sin bedömning i det konkreta fallet är tydligare med hur kravet om att konsumenten ska ha haft faktisk

lets karaktär (ingen möjlighet att påverka innehållet) och kundens underlägsna ställning jämte banken.

[41] Att fråga om bundenhet till kreditavtal som slutits genom obehörig användning av BankID inte faller inom 5 a kap. betaltjänstlagens tillämpningsområde framstår i sammanhanget som mindre problematiskt eftersom det i ett sådant fall inte alls handlar om en obehörig transaktion på kundens konto.

insikt om missbruksrisken som uppställs i p. 27 förhåller sig till den objektiverade bedömningen som beskrivs i p. 28. Hur effektivt konsumentskyddet blir kommer givetvis påverkas avsevärt av om man – vilket HD verkar göra i det aktuella målet – låter bedömningen bero på vad den aktuella konsumenten faktiskt förstått och hur agerandet mot denna bakgrund ska kvalificeras, eller om det istället är vad någon tänkt jämförelsekonsument hade förstått och hur denna istället kan förväntas ha agerat som ska avgöra.[42] Oavsett vilket är det tydligt att bedömningen måste göras konkret och mot bakgrund av att bevisbördan för att visa att kunden agerat särskilt klandervärt verkligen ligger på den kontoförvaltande banken, och att rent typiserade ansvarsbedömningar inte är vägen att gå.

Man *kan*, vilket jag nog är benägen att göra, uppfatta det så att HD:s bedömning i det konkreta fallet är uttryck för att HD anser att den aktuella konsumenten *hade* agerat såsom en tänkt jämförelsekonsument hade gjort. En sådan tolkning innebär visserligen risk för konstruktion och att man lägger ord i HD:s mun. Det som tyder på att tolkningen ändå kan vara rimlig, är (i) en förmodan om att HD inte avsett att skapa potentiellt motstridande bedömningsgrunder, (ii) att HD allmänt kan förväntas göra det den själv säger att den gör, åtminstone inom ramen för ett och samma avgörande och (iii) att domskälen i övrigt präglas av medvetenhet och att det finns flera exempel på att de mer allmänna skälen ska läsas i ljuset av den konkreta bedömningen och vice versa.

Bristen på en mer uttrycklig redovisning av hur bedömningen faktiskt gått till är emellertid fortsatt en svaghet, vilket kan tänkas få betydelse särskilt i två avseenden. För det första är möjligheterna att tolka HD:s domskäl och vad som egentligen menas väl stora. För det andra innebär det att vägledningen avseende hur denna bedömning ska gå till för senare fall är mer begränsad än den hade behövt vara. Bägge delar kan leda till en fortsatt osäker rättstillämpning och utmaningar för konsumenters möjlighet att i svåra fall *få rätt*. Att tröskeln för konsumentens ansvar i denna typ av mål överlag kommer att läggas högre idag än innan domen meddelades, är emellertid bortom tvivel.

Marianne M. Rødvei Aagaard

[42] Kanske är det vi ser här ett (omedvetet) uttryck för slitningen mellan den äldre nordiska och den EU-rättsliga uppfattningen om hur konsumentskydd bör utformas. I Norden har konsumentskydd traditionellt handlat om huruvida den aktuella personen är skyddsvärd, medan den EU-rättsliga tydligare tar avstamp i en genomsnittlig konsument som främst bara behöver nog med information för att kunna ta sina rättigheter tillvara.