

Obehöriga transaktioner. En konsument, som i samband med ett bedrägeri inte har skyddat sina personliga koder, anses ha agerat grovt oaktsamt (men inte särskilt klandervärt) och ska därför stå för endast en del av förlusten.

Beslut 2022-11-09; 2022-04140

HN begärde ersättning med 155 974 kr. I andra hand begärde han ersättning med 143 974 kr.

I sin anmälan till nämnden uppgav han följande. Han blev uppringd av en man som uppgav att han ringde från hans teleoperatör. Mannen presenterade sig med för- och efternamn, var mycket trevlig och gav ett professionellt intryck. Mannen sa att det hade blivit fel med hans fakturor så att en seniorrabatt inte hade dragits av. Han hade inte tidigare hört talas om någon seniorrabatt men kände igen principen från t.ex. Ica. Mannen behövde bekräfta ett antal uppgifter och läste upp hans namn, personnummer, mejladress, bankkontonummer och kontokortsnummer. Alla uppgifter var korrekta.

Därefter uppmanades han att gå in på bankens hemsida och logga in där med hjälp av sin bankdosa. Han var först tveksam till detta men mannen sa att han inte skulle behöva säga sin personliga kod till dosan utan endast svara på den kod som skickades till hans dosa. Sedan fick han veta att det enda som återstod var att han skulle godkänna utbetalningen genom att legitimera sig med sitt mobila BankID. Eftersom han inte kan koden till sitt mobila BankID kunde han inte logga in. Efter detta avslutades samtalet. Han minns inte om han gav mannen cvv-koden till sitt kort eller inte.

Dagen därpå såg han att utbetalningar hade gjorts från hans konto. Senare kom det dessutom fram att ett lån hade tagits i hans namn. Banken har återbetalat 50 000 kr till honom.

Efter två större och flera mindre stroker är han rullstolsburen och lider av hjärntrötthet. Han upplevde situationen som pressad.

Banken motsatte sig kravet.

I sitt svar till nämnden uppgav banken följande. Bankens tekniska utredning visar att HN har använt sin bankdosa tillsammans med sitt bankkort och att han har tagit instruktioner från den främmande mannen. HN har då knappat in den engångskod som han lär ha fått uppläst för sig och sedan har han bekräftat den med sin pinkod. Därefter har han för mannen uppgett den svarskod som bankdosa genererat. Processen har upprepats en andra gång. Svarskoderna som han lämnade ut användes för att legitimera HN hos banken och skapa ett nytt BankID, som användes för de aktuella transaktionerna.

Trots att HN enligt egna uppgifter är van att använda säkerhetslösningarna och medveten om att inga koder får lämnas ut, har han alltså följt den främmande personens instruktioner. Det förefaller dessutom märkligt att han skulle behöva ta fram sin bankdosa och lämna ut en svarskod för att få en återbetalning. Det var inte fråga om en pressad situation.

HN:s agerande är att betrakta som särskilt klandervärt.

Allmänna reklamationsnämnden gjorde följande bedömning.

Allmänt om regleringen

I lagen (2010:751) om betaltjänster finns regler om obehöriga transaktioner (se 5 a kap.). Huvudregeln är att kontohavarens betaltjänstleverantör (banken) ska återställa kontot till den ställning som det

skulle ha haft om den obehöriga transaktionen inte hade genomförts. Som utgångspunkt ska konsumenten alltså inte svara för någon del. Från denna regel finns emellertid vissa undantag. Undantagen hänger samman med att användaren är skyldig att skydda sina personliga behörighetsfunktioner, t.ex. koder, som är knutna till ett betalningsinstrument, t.ex. ett kreditkort, ett BankID eller en bankdosa. Kontohavaren är även skyldig att snarast anmäla till betaltjänstleverantören när kontohavaren känner till att betalningsinstrumentet har kommit bort eller obehörigen använts och att i övrigt följa de villkor som gäller för användning av betalningsinstrumentet enligt avtalet.

Kontohavaren ansvarar för hela beloppet, om han eller hon har agerat särskilt klandervärt. Ifall kontohavaren i stället har agerat grovt oaktsamt är ansvaret begränsat till 12 000 kr, om innehavaren är en konsument. Om kontohavaren varken har agerat särskilt klandervärt eller grovt oaktsamt, är ansvaret begränsat till 400 kr under förutsättning att de obehöriga transaktionerna har kunnat genomföras till följd av att kontohavaren inte har skyddat sin personliga behörighetsfunktion.

Som framgår är dessa regler tillämpliga när det handlar om transaktioner som är obehöriga i lagens mening. För att så ska anses vara fallet krävs att transaktionen har genomförts utan samtycke från kontohavaren eller någon annan som enligt kontoavtalet är behörig att använda kontot. Så kan fallet vara när kontohavaren förmås att genomföra en transaktion utan att förstå innebörden av detta.

Närmare om ansvarsgraderna

Om transaktionen är obehörig, ska kontohavaren själv svara för den ekonomiska förlusten under vissa förutsättningar. Det kräver bl.a. ett agerande som är grovt oaktsamt eller särskilt klandervärt. I fall av grov oaktsamhet är dock ansvaret, som tidigare framgått, begränsat till 12 000 kr om kontohavaren är konsument.

För att kontohavaren ska anses ha agerat grovt oaktsamt krävs att det är fråga om ett markant avsteg från normal aktsamhet och att agerandet därmed har varit obetänksamt i sådan grad att det inte kan ursäktas (se prop. 2009/10:122 s. 27).

Särskilt klandervärt får agerandet anses vara först vid kvalificerade former av grov oaktsamhet. Agerandet ska alltså vara allvarligare än ett markant avsteg från normal aktsamhet. Det ska närmast röra sig om fall där kontohavaren genom sitt handlande får anses ha varit likgiltig till risken för obehöriga transaktioner. I lagens förarbeten sägs att det obegränsade ansvaret tar sikte på situationer där konsumenten har agerat så pass klandervärt att det skulle vara stötande att banken behövde stå för någon del av beloppet (se prop. 2009/10:122 s. 29).

Det är banken som har bevisbördan för dessa omständigheter.

Ansvarsgraden får avgöras efter en nyanserad helhetsbedömning av omständigheterna i varje enskilt fall. I situationer där kontohavaren har låtit bli att skydda sina personliga behörighetsfunktioner i samband med ett bedrägeri bör särskilt avseende fästas vid vad kontohavaren har insett eller borde ha insett i fråga om risken för att funktionerna skulle användas för de obehöriga transaktioner som har ägt rum.

Agerandet får i regel anses särskilt klandervärt i fall där kontohavaren lämnar ut sina personliga behörighetsfunktioner till någon och samtidigt dels är medveten om att det rör sig om en obehörig person, dels inser eller har anledning att misstänka att det föreligger en betydande eller närliggande risk för att handlandet kan medföra en förlust. Ett obegränsat ansvar får även anses föreligga i situationer där kontohavaren faktiskt insåg att det fanns en risk för en obehörig transaktion men ändå lät bli att skydda sina personliga behörighetsfunktioner (se rättsfallet NJA 2022 s. 522 "BankID-bedrägeriet").

Om något av dessa kriterier är uppfyllt, får kontohavaren nämligen normalt sett anses ha varit likgiltig till risken för de obehöriga transaktionerna och agerandet får därmed bedömas som särskilt klandervärt såvida inte tungt vägande motstående intressen föranleder att det ändå inte kan anses vara stötande att kontohavaren inte ansvarar för förlusten i dess helhet.

I fall där kontohavaren inte har varit likgiltig till risken för de obehöriga transaktionerna, t.ex. för att han eller hon inte insåg ens att det fanns en risk för en sådan transaktion, kan agerandet i allmänhet inte bedömas som särskilt klandervärt. Men om kontohavaren har haft anledning att räkna med risken för en obehörig transaktion, kan agerandet anses ha varit grovt oaktsamt.

I den situationen, dvs. vid bedömningen av om kontohavaren kan anses ha agerat grovt oaktsamt, måste man beakta vad han eller hon hade kunnat göra för att komma till insikt om hur det faktiskt förhöll sig och ta ställning till om det kan begäras att han eller hon gör detta. I det sammanhanget kan många olika faktorer få betydelse. Bland dessa ingår individuella faktorer såsom ålder, erfarenhet, fysiska egenskaper och stresstolerans. Det får även betydelse hur förslaget bedrägeriet har varit och hur pressande eller brådskande situationen har varit eller uppfattats. Här bör hänsyn tas till hur bedragaren har framstått, om personen har varit förtroendeingivande eller om det i stället har funnits förhållanden som normalt sett bör ge anledning till misstanke. Hänsyn ska även tas till karaktären av de uppgifter som lämnas ut och det sätt på vilket detta har skett.

Faktorer av det här slaget påverkar både kontohavarens möjligheter att ta reda på om det finns en risk för obehöriga transaktioner och vad som kan krävas av honom eller henne i det avseendet. Ytterst får dessa och andra liknande omständigheter vägas samman för att avgöra om kontohavaren kan klandras för att inte ha skaffat sig kunskap om hur det förhöll sig. Om så är fallet, kan agerandet anses ha varit grovt oaktsamt under förutsättning att underlåtenheten dessutom kan anses utgöra ett mycket tydligt avsteg från normal aktsamhet och inte är en följd av exempelvis ett inte särskilt allvarligt fall av obetänksamhet, slarv, oförstånd eller godtrogenhet.

Nämndens bedömning

Av utredningen i ärendet framgår att HN blev uppringd av en man som felaktigt utgav sig för att ringa från hans teleoperatör. Han lurades att tro att han skulle tillgodoräknas en seniorrabatt och att han behövde logga in på sin internetbank och där godkänna utbetalningen genom att legitimera sig med sitt BankID. Det framgår av utredningen att svars-koder från hans säkerhetsdosa användes för att skapa ett nytt BankID, som användes för att genomföra de aktuella transaktionerna. Det får därmed anses utrett att HN lämnade ut svars-koder från sin säkerhetsdosa till bedragaren. Det står således klart att HN inte har skyddat de personliga behörighetsfunktioner som har varit knutna till hans säkerhetsdosa och att transaktionen kunde genomföras till följd av denna underlåtenhet.

Det är även utrett att bedragaren genomförde transaktionerna utan att HN hade samtyckt till detta. Det rör sig alltså om obehöriga transaktioner.

Frågan är härefter om HN:s underlåtenhet att skydda svars-koderna har varit särskilt klandervärd eller grovt oaktsamt.

HN lämnade ut svars-koderna till en person som utgav sig för att ringa från hans teleoperatör. Det står därmed klart att han var medveten om att personen inte var behörig att hantera hans uppgifter. Det får visserligen antas att han då inte insåg att det fanns en stor sannolikhet att uppgifterna skulle missbrukas. Att avslöja den typen av uppgifter för en okänd person på det sätt som har skett måste emellertid anses förknippat med en påtaglig fara för obehörig användning. Det måste rimligen krävas att man inser detta.

Slutsatsen blir därför att HN med avsikt har lämnat över personliga behörighetsfunktioner till en obehörig person och att han samtidigt hade anledning att misstänka att det förelåg en betydande eller närliggande risk för att hans handlande kunde medföra en förlust. Samtidigt måste beaktas att HN, som vid tillfället var 76 år gammal, har drabbats av flera strokes och lider av funktionsnedsättningar. Vid en sammantagen bedömning av det som har kommit fram om hans personliga förhållanden kan det enligt nämndens mening inte rimligen krävas att han skulle inse hur påtaglig faran för missbruk var. Nämnden bedömer därför att HN:s agerande inte kan anses ha varit särskilt klandervärt.

Frågan blir då om HN:s agerande ska bedömas som grovt oaktsamt.

Som framgår måste det anses förknippat med en påtaglig fara för obehörig användning att avslöja sina svarskoder för en obehörig person. Genom att göra detta får HN på ett mycket tydligt sätt anses ha avvikit från den aktsamhet som kan krävas av honom. Det kan visserligen inte begäras att HN skulle inse omfattningen av den risk för missbruk som förelåg, men han borde ändå ha förstått att det fanns en beaktansvärd risk för obehöriga transaktioner. Avvikelsen från den aktsamhet som rimligen kan krävas är vid dessa förhållanden så pass allvarlig att HN får anses genom grov oaktsamhet ha försummat skyldigheten att skydda sin personliga behörighetsfunktion.

HN:s ansvar är alltså begränsat till 12 000 kr. Med avdrag för detta belopp ska därför banken rekommenderas att ersätta den förlust som de obehöriga transaktionerna har orsakat honom.

Skiljaktiga meningar

Två ledamöter är skiljaktiga i fråga om motiveringen till nämndens beslut och anförde följande.

Högsta domstolen har tagit ställning till vad som utgör särskilt klandervärt respektive grovt oaktsamt handlande i en dom om betalningsansvaret vid obehöriga transaktioner där konsumenten hade lämnat ut svarskoder från sin bankdosa till en bedragare (NJA 2022 s. 522).

Högsta domstolen konstaterade att agerandet får anses vara särskilt klandervärt om 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 (p. 26).

Utöver dessa fall får det anses vara särskilt klandervärt när konsumenten – även om han eller hon inte avskiltligen överlämnade en personlig behörighetsfunktion till någon obehörig – var likgiltig till risken för obehöriga transaktioner. Ett särskilt klandervärt agerande föreligger alltså om 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 § betaltjänstlagen. Vid denna bedömning får det särskild betydelse till vem han eller hon uppfattade att den personliga behörighetsfunktionen lämnades ut (p. 27).

Högsta domstolen uttalade vidare att bedömningen av om en konsument har agerat särskilt klandervärt ska i princip göras objektiverat, dvs. utifrån hur en konsument av motsvarande slag i samma situation typiskt sett skulle ha agerat. Vid bedömningen av ett eventuellt ansvar när konsumenten i samband med ett bedrägeri inte har skyddat sina personliga behörighetsfunktioner knutna till betalningsinstrumentet finns det anledning att fästa särskild vikt vid vissa faktorer. Bland dessa ingår den miljö och situation som konsumenten befann sig i samt hans eller hennes möjlighet att skydda sig mot en obehörig transaktion. Konsumentens ålder och

erfarenhet kan vara av betydelse. Vidare bör hänsyn tas till hur förslaget bedrägeriet har varit och till vad konsumenten förstått eller borde ha förstått om de uppgifter som lämnades ut och de möjliga konsekvenserna av att de lämnades ut (p. 28).

Det är betaltjänstleverantören som har bevisbördan för att konsumenten har handlat särskilt klandervärt.

Av utredningen i ärendet framgår att HN blev lurad att lämna ut tre svars-koder från sin säkerhetsdosa till en person som uppgav sig ringa från Telia. Personen sa att något blivit fel med hans fakturor så att en seniorrabatt inte dragits av. Personen lämnade instruktioner för hur rabatten kunde aktiveras och uppmanade HN att gå in på bankens hemsida och logga in där med hjälp av sin bankdosa. Han blev sedan uppmanad att lämna ut svars-koder från bankdosan. Koderna användes för att skapa ett nytt BankID i HN:s namn. Det nya BankID:et användes sedan för att genomföra de reklamerade transaktionerna.

Det är utrett att bedragaren genomförde transaktionerna utan att HN hade samtyckt till detta. Det rör sig alltså om obehöriga transaktioner.

Frågan är här efter om HN:s utlämnande av svars-koder till bedragaren per telefon i den aktuella situationen inneburit att han åsidosatt sin skyldighet att skydda sina personliga behörighetsfunktioner genom grov oaktsamhet och om han dessutom handlat särskilt klandervärt.

Vi konstaterar inledningsvis att det strider mot bankens villkor att lämna ut personliga behörighetsfunktioner i form av personliga koder på det sätt som skett i ärendet. Motsvarande villkor förekommer hos praktiskt taget alla svenska banker. Mot denna bakgrund får det anses vara allmänt känt att en bankkund inte får lämna ut sina personliga koder till någon.

Varje muntligt utlämnande av personliga behörighetsfunktioner innebär alltså, objektivt sett, ett utlämnande till en obehörig person.

Att lämna ut koder till en obehörig person ”med avsikt” får anses innebära ett utlämnande med insikt om att det sker till en obehörig person.

I sammanhanget bör beaktas att det numera är mycket vanligt med bedrägeriförsök där kunden kontaktas av en bedragare som försöker lura kunden att lämna ut personliga koder för att t.ex. spärra konton och kort eller på annat sätt skydda kundens tillgångar. Detta har uppmärksammats vid ett stort antal tillfällen i media.

Personliga koder som genereras från bankdosor används för att godkänna betalningar och andra digitala rättshandlingar mot banken. En kund som brukar genomföra betalningar med bankdosa vet därför typiskt sett att det finns en risk för en obehörig transaktion om dessa koder lämnas ut till en okänd person.

Mot denna bakgrund får bankkunder i allmänhet anses känna till att personliga koder inte får lämnas ut.

Vid den objektiverade bedömning som ska göras av kundens agerande och insikt i det enskilda fallet ska särskilt avseende fästas vid de faktorer som framgår av p. 28 i domskälen i rättsfallet NJA 2022 s. 522.

HN lämnade ut koderna från bankdosa till en person som påstod sig ringa från Telia. Att lämna ut koderna till en sådan person kan endast under mycket särskilda omständigheter, dvs. rena undantagsfall, anses ha skett utan insikt om att koderna lämnades ut till en obehörig person.

Bedragaren uppgav att HN behövde lämna ut koder från bankdosa för att hans faktura från Telia skulle krediteras med ett visst belopp. Det var alltså inte en pressad situation. Det är vidare utrett att HN är van att använda sin bankdosa och medveten om att inga koder får lämnas ut. HN har inte lämnat någon förklaring till varför han trodde att det var tillåtet att lämna ut koderna till en företrädare för Telia i detta fall eller varför han behövde logga in på bankens hemsida.

Utredningen visar att det inte var fråga om ett förslaget bedrägeri.

Det är dock utrett i målet genom uppgifter från HN:s ombud att HN drabbats av flera strokes, att han vid tidpunkten för den aktuella händelsen led av hjärntrötthet och att en förvaltare enligt föräldrabalken numera är förordnad för honom.

Vi bedömer därför att han får antas ha haft begränsade möjligheter att göra en adekvat bedömning av situationen.

Det är därför inte bevisat att HN avsiktligt lämnade ut koderna till en obehörig person.

Det får inte heller anses bevisat att han var medveten om, dvs. faktiskt insåg, att det fanns en risk för obehöriga transaktioner när han lämnade ut sina personliga koder

HN:s handlande är alltså inte att bedöma som särskilt klandervärt.

Vi delar majoritetens bedömning att HN får anses ha försummat skyldigheten att skydda sina personliga behörighetsfunktioner genom ett grovt oaktsamt agerande.

En ledamot är skiljaktig i fråga om motiveringen till nämndens beslut och anförde följande.

Det står klart att HN förmått att lämna ut svars-koder från sin säkerhetsdosa till en bedragare, vilket lett till att bedragaren kunnat göra transaktioner från hans konto. Det står vidare klart att transaktionerna genomförts utan HN:s samtycke, vilket medför att transaktionerna är att betrakta som obehöriga. HN har inte skyddat de personliga behörighetsfunktioner som varit knutna till hans konto, vilket lett till att de aktuella transaktionerna har kunnat genomföras. Frågan är om HN genom grov oaktsamhet har åsidosatt sin skyldighet att skydda de personliga behörighetsfunktionerna.

Det får normalt anses förenat med risker att överlämna svars-koder till någon annan. Därför får det i regel krävas att man ifrågasätter behovet av att överlämna uppgifter på det sätt som har skett och att man gör vad man kan för att kontrollera vem man överlämnar koderna till i en situation som denna. Genom att lämna ut svars-koderna till bedragaren får HN anses ha avvikit från den aktsamhet som rimligen kan krävas av honom. Han har således genom grov oaktsamhet försummat skyldigheten att skydda sina personliga behörighetsfunktioner.

Frågan är härefter om HN har agerat särskilt klandervärt.

Utredningen visar inte annat än att HN trodde att han lämnade svars-koder från sin säkerhetsdosa till en person i syfte att han skulle erhålla en seniorrabatt hos sin teleoperatör. Banken har inte

bevisat att HN avsiktligt överlämnade svarskoder till en obehörig person. Banken har inte heller visat att HN insåg att det fanns en risk för att personen skulle genomföra de transaktioner som kom att ske. Banken har därmed inte bevisat att HN har varit likgiltig till risken för obehöriga transaktioner. Slutsatsen blir därför att HN inte kan anses ha agerat särskilt klandervärt. Han ansvarar således inte för hela förlusten utan hans ansvar är begränsat till 12 000 kronor av förlusten. Med avdrag för detta belopp ska banken därför rekommenderas att ersätta den förlust som den obehöriga transaktionen har orsakat honom.