Obehöriga transaktioner. Konsumenten blev först uppringd av en person som utgav sig för att företräda en bank där han inte hade något konto. Han blev därefter kopplad till en man som utgav sig för att företräda hans bank. Denne skulle ordna med en brandvägg till hans wifi-anslutning. Han fick ett varningsmeddelande när han signerade nedladdningen av ett nytt BankID, han gav mannen tillgång till sin datorskärm genom en fjärrstyrning och han höjde betalgränsen för Swish. ARN har bedömt att det är otänkbart att konsumenten inte i samband med i vart fall något av de skeenden som föregick transaktionen blev medveten om att det fanns en risk för den obehöriga transaktion som kom att genomföras. Konsumentens handlande var därför särskilt klandervärt.

Beslut 2023-12-13; 2022-21906

RH begärde ersättning med 98 800 kr.

I sin anmälan till nämnden uppgav RH följande. Den 2 augusti 2022 blev han uppringd av en person som sade sig ringa från säkerhetsavdelningen på en bank. Enligt personen som ringde hade han haft intrång på sitt konto samma dag. Han svarade att han inte hade något konto hos banken utan hos en annan bank. Han blev då kopplad till säkerhetsavdelningen hos sin egen bank. Där förklarade man att han hade blivit utsatt för falska uttag och att han skulle få hjälp med att ordna en brandvägg till sitt wifi. De skulle dessutom försöka föra tillbaka de falska uttagen. Vid samtalet underströk han att han hade säkerhetsprogram. Han fick svaret att han även måste ha en brandvägg för sitt wifi. Han blev stressad och följde den uppringandes instruktioner. Han fick en länk med AnyDesk skickad till datorn. Han uppmanades att klicka på länken och identifiera sig med BankID via QR-kod. För att få tillgång till brandväggen behövde han bekräfta med BankID flera gånger. Mannen vid banken hade därmed tagit över hans dator. Han misstänkte fortfarande inget, allt verkade trovärdigt för honom. Mannen som ringde var förtroendeingivande och verkade tekniskt kunnig.

På uppmaning av en anhörig ringde han upp sin personlige bankman, dock utan att få svar. Direkt därefter fick han ett sms från sin bank som uppmanade honom att genast ringa. När han gjorde det visade det sig att han hade blivit lurad och att det skett flera obehöriga transaktioner på flera konton. Totalt förlorade han 98 800 kr.

Han har uppfattat sig själv som ganska medveten om den här typen av hot. Trots det misstänkte han inget under samtalet. Han kopplade samtalet till ett stort antal mejl med förslag på säkerhetsprogram och uppgifter om att hans förhållanden cirkulerade på internet.

Banken motsatte sig kravet.

I sitt svar till nämnden uppgav banken följande. RH har agerat på ett sätt som inte bara är att anse som grovt oaktsamt, utan även särskilt klandervärt i betaltjänstlagens mening.

Av bankens utredning framgår att den transaktion som är föremål för prövning hos nämnden är signerad med ett BankID som RH under händelseförloppet laddade ned till bedragarens enhet. Inledningsvis legitimerade sig RH mot banken och höjde betalgränsen för Swish. Därefter signerade han flertalet banköverföringar. Sedan signerade han nedladdning av det nya BankID:t. Samtliga dessa åtgärder signerades med RH:s befintliga BankID i hans mobiltelefon. Han gjorde det möjligt för bedragaren att ladda ned det nya BankID:t till sin enhet genom att dela sin skärm så att bedragaren kunde skanna en QR-kod. Slutligen genomförde bedragaren Swish-transaktionen om 98 800 kr med det nya BankID:t.

Betaltjänstanvändaren är skyldig att noggrant granska vad som presenteras för signering vid godkännande av en betalningstransaktion. Användaren är ansvarig för skada eller förlust som åsamkas banken, tredje man eller sig själv om användaren uppsåtligen eller genom oaktsamhet inte iakttar villkoren. BankID får exempelvis bara laddas ned till en enhet som betaltjänstanvändaren har kontroll över.

RH har i sin redogörelse för händelsen uppgett att han blev uppringd av en person som påstod sig ringa från en annan bank än hans egna. RH rättade då bedragarens uppenbara misstag genom att förklara att han inte har något engagemang i en annan bank, utan i sin egen. Bedragaren förklarade då att han ”kopplade” RH till hans bank i stället. Redan i det skedet borde RH ha förstått att det rörde sig om ett bedrägeri. Hur en annan bank skulle ha fått kännedom om att han hade haft intrång på sina konton i sin bank är oklart. Vidare måste det ha framstått som märkligt att en annan bank skulle koppla honom till sin egen bank. RH lät sig emellertid kopplas och följde den okända personens instruktioner. Den nya personen instruerade RH i att ladda ned ett program till sin dator, höja betalgränsen för Swish, signera totalt fem banköverföringar och ladda ned ett nytt BankID till bedragaren.

Att banken skulle be RH att ladda ned ett program på sin dator förefaller så udda att han senast vid den tidpunkten borde ha avslutat samtalet och själv ringt till bankens kundtjänst för att kontrollera att allting var i sin ordning. Det gjordes ingen ansats för att försäkra sig om att han var i kontakt med banken. Han hade ingen anledning att anta att personen han pratade med var en representant för banken. Tvärtom hade han all anledning att ifrågasätta detta. I stället för att kontrollera detta följde RH den okända personens instruktioner och laddade inledningsvis ned ett för honom främmande program på sin dator. Att ett program laddades ned till datorn saknar betydelse för bedömningen av RH:s möjligheter att uppfatta vilka åtgärder han signerade eftersom dessa genomfördes med hans mobila BankID i hans mobiltelefon. Det står emellertid klart att det nya BankID:t inte hade kunnat laddas ned till bedragarens enhet utan att RH installerade programmet och delade sin skärm med bedragaren så att bedragaren kunde skanna den QR-kod som krävs för att fullfölja nedladdningen till en ny enhet. En QR-kod skannas i enheten med det befintliga BankID:t vid inloggning i steg 2 och en ny QR-kod skannas i den nya enheten i steg 6. Vidare står det klart att AnyDesk har ett tydligt varningsmeddelande i samband med nedladdning om att aldrig ge en främmande person tillgång till sin egen enhet, tillsammans med en länk där användaren kan läsa mer om hur man undviker att bli utsatt för bedrägeri.

RH möjliggjorde sedan den Swish-transaktion som senare ägde rum, genom att själv höja betalgränsen för Swish till 100 000 kr. Han fick en tydlig upplysning om vad det var han signerade. Följande meddelande visades i hans BankID-app.

Jag vill ha en tillfällig limit i Swish tillfällig limit: 100 000,00 SEK giltig till: 2022-08-02

Efter att den nya betalgränsen för Swish var signerad använde RH åter sitt BankID för att signera banköverföringar. Även vid samtliga dessa tillfällen fick han tydliga upplysningar i sin BankID-applikation om vad det var han signerade. Meddelandena såg ut som följande.

Jag vill betala belopp: 18 500,00 SEK
mottagare: Trustly Group AB
*till konto: 48*******82*
datum: 2022-08-02
*från konto: 30*******97*

Det framgår inte av RH:s redogörelse för händelsen varför han skulle ladda ned ett nytt BankID. Bankens utredning visar att han återigen fick en tydlig upplysning om att han signerade en sådan

åtgärd med sitt BankID. Till upplysningen fick RH även en tydlig varning om att aldrig ladda ned ett nytt BankID på uppmaning av någon annan, inte ens en person som han uppfattar som representant för banken. När RH signerade nedladdningen av det nya BankID:t fick han följande meddelande.

> *Jag vill ladda ner ett nytt BankID. Jag har tagit del av och godkänner Allmänna villkor för BankID. UNDVIK BEDRÄGERIFÖRSÖK! Ladda aldrig ner ett BankID på uppmaning av banken eller någon annan person, oavsett orsak! Vid minsta tvekan, 'Avbryt'*

Banken har sålunda uppmanat RH att inte genomföra precis den åtgärd han ändå valde att genomföra. Det nya BankID:t laddades i strid med såväl bankens villkor som betaltjänstlagen ned till en enhet han inte hade kontroll över. Uppmaningen gav även RH ytterligare skäl att anta att han inte var i kontakt med banken. Banken är tydlig med att inga sådana förfrågningar kommer från banken. Hade RH inte tillåtit skärmdelning av sin dator hade bedragaren inte kunnat skanna den sista QR-koden och slutföra nedladdningen.

Att använda sitt BankID på det sätt som har skett måste anses vara förknippat med en påtaglig fara för obehöriga transaktioner och det måste rimligen krävas att man inser detta. RH kringgick skyddet med QR-kod genom att ladda ned en programvara som delade hans skärm med bedragaren. Han ignorerade varningsmeddelandet vid nedladdning av det nya BankID:t och signerade detsamma trots meddelandet. Han kringgick sedan skyddet som hindrade bedragaren från att höja betalgränsen för Swish genom att själv höja gränsen med sitt befintliga BankID. Allt detta gjorde han efter att först ha signerat flertalet banköverföringar med tydliga upplysningar om att signeringarna skulle innebära att pengar drogs från hans konto, vilka inleddes med ”Jag vill betala […]”. Att hans handlande skulle komma att medföra förlust stod således klart.

Slutsatsen blir därför att RH med avsikt har gett en obehörig person tillgång till sina personliga behörighetsfunktioner och att han samtidigt hade anledning att misstänka att det förelåg en betydande eller närliggande risk för att hans handlande skulle medföra en förlust.

Banken gör således gällande att RH på ett särskilt klandervärt sätt försummat skyldigheten att skydda sin personliga behörighetsfunktion. Banken har därför ingen skyldighet att återställa kontot. Banken lyckades återboka de behöriga transaktionerna. Den omständigheten saknar dock betydelse för ansvarsfrågan.

Allmänna reklamationsnämnden gjorde följande bedömning.

Reglerna om obehöriga transaktioner

I lagen (2010:751) om betaltjänster finns regler om obehöriga transaktioner. Huvudregeln är att banken ska återställa kontot till den ställning som det skulle ha haft om den obehöriga transaktionen inte hade ägt rum. Från denna regel finns emellertid undantag, som hänger samman med att kontohavaren är skyldig att skydda sina personliga behörighetsfunktioner, t.ex. koder, som är knutna till ett betalningsinstrument.

Kontohavaren ansvarar för obehöriga transaktioner under förutsättning att transaktionen har kunnat genomföras till följd av att kontohavaren inte har skyddat sin personliga behörighetsfunktion. Ansvaret är emellertid begränsat till 400 kr, om inte kontohavaren har agerat grovt oaktsamt eller särskilt klandervärt. Om kontohavaren är konsument och har låtit bli att skydda sina personliga behörighetsfunktioner genom grov oaktsamhet, gäller ansvaret i stället upp till 12 000 kr. Och i de fall

där handlandet ska anses vara särskilt klandervärt, ansvarar kontohavaren för hela förlusten oavsett hur stor den är. (Se 5 a kap. 2 § och 3 § andra stycket.)

Regleringen bygger på tanken att det ligger ett värde i att man kan använda kontokort och andra betalningsinstrument utan att riskera att drabbas av alltför kännbara ekonomiska förluster. Det har nämligen ansetts vara önskvärt att uppmuntra användningen av betalningsinstrument eftersom det finns ett samhällsekonomiskt och brottsförebyggande intresse av att minska kontanthanteringen. (Se prop. 2009/10:122 s. 17.)

Grovt oaktsamma ageranden

För att vara grovt oaktsamt måste agerandet utgöra ett markant avsteg från den aktsamhet som rimligen kan krävas. Normalt förutsätts därmed att kontohavaren har varit obetänksam i en sådan grad att han eller hon inte är ursäktad. Detta innebär att lindriga fall av slarv eller tillfällig glömska inte utgör ett grovt oaktsamt agerande. Vid bedömningen måste beaktas bland annat vilka möjligheter kontohavaren har haft att skydda sig mot en obehörig transaktion. I det sammanhanget ska hänsyn tas till vad han eller hon hade kunnat göra för komma till insikt om risken för en obehörig transaktion. Ställning måste vidare tas till om det är rimligt eller inte att begära att kontohavaren gör detta. I det sammanhanget kan många olika faktorer ges betydelse, däribland hur pressande eller brådskande situationen har varit eller framstått för honom eller henne. Ytterst får en samlad bedömning göras för att avgöra om agerandet kan anses grovt oaktsamt eller inte. (Se prop. 2009/10:122 s. 27 samt nämndens beslut den 9 november 2022 i ärendena 2021-12666, 2021-19593, 2022-01950, 2022-02184, 2022-03987 och 2022-03828.)

Särskilt klandervärda ageranden

Särskilt klandervärt ska agerandet anses vara först vid kvalificerade former av grov oaktsamhet. Agerandet ska alltså vara allvarligare än ett markant avsteg från normal aktsamhet (se ovan). I princip krävs att konsumenten har varit likgiltig till risken för obehöriga transaktioner (se prop. 2009/10:122 s. 29).

Högsta domstolen har nämnt tre situationer där agerandet ska anses vara särskilt klandervärt. Den första av dessa är när konsumenten har agerat bedrägligt. Den andra situationen föreligger när konsumenten med avsikt har överlämnat personliga behörighetsfunktioner till en obehörig person och då insett eller haft anledning att misstänka att det förelåg en betydande eller närliggande risk för att hans eller hennes handlande kunde medföra en förlust. För det tredje nämner domstolen situationen att konsumenten har varit medveten om, dvs. faktiskt insett, att det fanns en risk för en obehörig transaktion men ändå underlåtit att skydda sina personliga behörighetsfunktioner. Bedömningen av om en konsument har agerat särskilt klandervärt ska i princip göras objektiverat. (Se ”BankID-bedrägeriet” NJA 2022 s. 522 punkterna 26–28.)

Det ska noteras att kravet på insikt gäller kontohavarens faktiska uppfattning eller föreställning om risken för att en obehörig transaktion ska genomföras. Det kan inte anses tillräckligt att kontohavaren anar att en sådan risk finns. I stället får det krävas att kontohavaren är mer eller mindre säker på att en verklig risk föreligger. Det är heller inte tillräckligt att kontohavaren borde ha insett risken eller har haft anledning att tänka efter och därmed hade kunnat inse att en sådan risk förelåg.

Bankens bevisbörda

Det är banken som har bevisbördan för att kontohavaren har agerat grovt oaktsamt eller särskilt klandervärt. Bevisningens styrka ska i princip uppfylla de krav som normalt gäller i civilmål; omständigheterna ska alltså visas. (Se prop. 2009/10:122 s. 28 och ”BankID-bedrägeriet” NJA 2022 s. 522 punkten 29.)

Vad banken närmare bestämt ska visa är att omständigheter av omedelbar betydelse för bedömningen föreligger som utgör ett grovt oaktsamt eller ett särskilt klandervärt agerande, t.ex. att kontohavaren var praktiskt taget säker på att det fanns en risk för obehöriga transaktioner. Det ska samtidigt uppmärksammas att bedömningen huruvida ett agerande är grovt oaktsamt eller särskilt klandervärt kan inrymma rättsfrågor och att frågor av det slaget inte omfattas av bevisbördan, t.ex. frågan om kontohavaren har haft anledning att misstänka att det förelåg en betydande eller närliggande risk för att hans eller hennes handlande kunde medföra en förlust.

Beviskravet kan uppfyllas på olika sätt och genom bevisning som tar sikte på olika omständigheter. I regel kan banken lägga fram utredning som gäller användningen av ett betalningsinstrument. Denna kan många gånger innehålla uppgifter om vilket betalningsinstrument som har använts, hur detta har kommit till användning och när användningen har ägt rum. I övrigt får nämnden inte sällan lägga kontohavarens uppgifter till grund för bedömningen, något som också förutsattes i lagmotiven (se prop. 2009/10:122 s. 28). Många gånger finns det således inte någon bevisning som mera direkt tar sikte kontohavarens subjektiva föreställning. Någon gång kan emellertid omständigheterna objektivt sett vara sådana att det framstår som i det närmaste otänkbart att kontohavaren var okunnig om risken för en obehörig transaktion (jfr ”Suterränghuset på Ekerö” NJA 2021 s. 353 punkten 11).

Nämndens bedömning i detta fall

RH har förklarat att han pratade med en person som utgav sig för att företräda banken och att han under samtalet använde sitt BankID flera gånger. Han har vidare förklarat att personen tog över hans dator med hjälp av en länk till fjärrstyrningsprogrammet AnyDesk som RH fick. Av den utredning som banken har lagt fram framgår att RH med sitt BankID signerade nedladdningen av ett nytt BankID och att han genom fjärrstyrningen delade sin skärm så att personen kunde skanna en QR-kod. På det sättet kunde personen ladda ned ett nytt BankID och använda detta för att genomföra den aktuella transaktionen.

Det står klart att RH inte själv genomförde transaktionen och att den gjordes utan hans samtycke. Det är vidare utrett att transaktionen kunde genomföras för att RH signerade nedladdningen av ett nytt BankID och gav tillgång till den QR-kod som visades på hans datorskärm. Transaktionen är alltså obehörig men kunde genomföras för att RH inte skyddade de personliga behörighetsfunktioner som var kopplade till hans BankID.

Frågan är om RH genom dessa åtgärder ska anses ha agerat särskilt klandervärt.

Av utredningen framgår att samtalet med den förmente bankföreträdaren föregicks av att RH blev uppringd av någon som utgav sig för att ringa från säkerhetsavdelningen på en annan bank än hans egna och som förklarade att RH hade haft intrång på sitt konto. När RH förklarade att han inte hade något konto hos den banken kopplades han vidare för att få prata med någon på den bank, där RH var kund.

Det framstår enligt nämnden som besynnerligt att en företrädare för en bank där RH inte hade något konto kontaktade honom och kopplade honom vidare till hans bank. Detta utgör emellertid inte i sig

tillräcklig bevisning för att RH var medveten om att den person som han röjde uppgifterna för var obehörig eller för att det fanns en risk för obehöriga transaktioner.

Av utredningen framgår därtill att RH, när han signerade nedladdningen av ett nytt BankID, fick ett meddelande som uppmanade honom att aldrig ladda ned ett BankID på uppmaning av banken eller någon annan person, oavsett orsak. Det har emellertid inte framkommit någon omständighet som mera direkt talar för att RH tog del av informationen.

Av utredningen framgår vidare att den förmente företrädaren för banken förklarade att han skulle hjälpa RH att ordna med en brandvägg till hans wifi-anslutning. Det framgår även att RH höjde betalgränsen för Swish till 100 000 kr och att han i samband med detta i sitt BankID fick information om att han godkände en höjning av betalgränsen. Det har inte framkommit någon förklaring till varför en sådan åtgärd enligt RH:s uppfattning var nödvändig. Enligt nämndens bedömning framstår det dessutom som främmande att banken skulle ordna med en brandvägg till hans wifi-anslutning.

Även om de redovisade omständigheterna tagna för sig inte utgör tillräcklig bevisning framstår det vid en sammantagen bedömning som i det närmaste uteslutet att RH inte förstod att det fanns en beaktansvärd risk för att han utsattes för ett bedrägeri. Det får nämligen anses vara otänkbart att han inte i samband med i vart fall något av de skeenden som föregick transaktionen blev medveten om att det fanns en risk för den obehöriga transaktion som kom att genomföras. Nämnden gör mot den bakgrunden bedömningen att det är styrkt att RH faktiskt insåg att det fanns en sådan risk. RH har därmed försummat skyldigheten att skydda sina personliga behörighetsfunktioner på ett särskilt klandervärt sätt. Hans krav ska därför avslås.

_____

Skiljaktig mening

Två av ledamöterna var skiljaktiga och gjorde följande bedömning.

Det står klart att RH av en bedragare förmåtts att ladda ned ett program som möjliggjorde för en bedragare att fjärrstyra hans dator. Det står vidare klart att RH signerat nedladdning av ett nytt Mobilt BankID till bedragarens enhet vilket lett till att bedragaren kunnat göra transaktioner från RH:s konto. Det står även klart att transaktionerna genomförts utan RH:s samtycke vilket medför att transaktionerna är att betrakta som obehöriga. RH har därmed inte skyddat de personliga behörighetsfunktionerna som varit knutna till hans konto vilket lett till att de aktuella transaktionerna kunnat genomföras. Frågan är därmed om RH genom grov oaktsamhet har åsidosatt sin skyldighet att skydda de personliga behörighetsfunktionerna.

RH har signerat nedladdningen av ett nytt Mobilt BankID och låtit en bedragare fjärrstyra hans dator. Det får normalt anses förenat med risker att låta någon fjärrstyra en dator samtidigt som man hanterar koder och andra behörighetsfunktioner som man därmed riskerar att avslöja. I aktuellt fall kan det också noteras att bedragaren inledningsvis uppgav att denne ringde från en bank som RH vid det aktuella tillfället inte hade något konto i. Detta i kombination med att bedragaren angav att denne skulle ordna med en brandvägg till RH:s wifi-anslutning gör att han borde ha reagerat och ifrågasatt behovet av sådana åtgärder. Trots att RH trodde att han var i kontakt med en representant från banken får han, mot bakgrund av dessa omständigheter, 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 RH:s agerande dessutom är särskilt klandervärt. Utredningen ger inte stöd för annat än att RH trodde att han, i kontakt med sin bank, godkände nedladdningen av ett

säkerhetsprogram. RH har hela tiden trott att hans agerande skulle medföra att de falska uttagen som gjorts från hans konto skulle återföras. Som framgår av NJA 2022 s. 522 krävs det för att en konsument ska få stå för hela beloppet för en obehörig transaktion att denne avsiktligen lämnat uppgifter till en obehörig person och då insåg eller hade anledning att misstänka att det förelåg en betydande eller närliggande risk för att dennes handlande kunde medföra en förlust. Konsumenten får även stå för hela förlusten om denne var medveten om, dvs. faktiskt insåg, att det förelåg en risk för en obehörig transaktion men trots detta agerade i strid med sina skyldigheter. Det är banken som har att bevisa detta.

Banken har inte bevisat att RH avsiktligen överlämnat en personlig behörighetsfunktion till en obehörig person. Banken har heller inte visat att RH insåg att det fanns en risk för att personen skulle genomföra de transaktioner som kom att ske.

Banken har således inte bevisat att RH har 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 därför banken rekommenderas att ersätta den förlust som den obehöriga transaktionen har orsakat honom.