Obehöriga transaktioner. Konsumenten hade fått ett s.k. spoofat sms med information om att banken misstänkte bedräglig aktivitet på hennes konto. Hon ombads kontakta bankens spärrservice på ett angivet telefonnummer, vilket hon gjorde. På uppmaning av den påstådda banktjänstepersonen laddade hon ned ett fjärrstyrningsprogram och signerade nedladdningen av ett nytt BankID. ARN har bedömt att konsumentens agerade var grovt oaktsamt (men inte särskilt klandervärt) eftersom hon, trots att hon hade fått ett tydligt och kortfattat varningsmeddelande, signerade nedladdningen av ett nytt BankID.

Beslut 2023-12-13; 2022-22360

HS begärde ersättning med 290 846 kr.

I sin anmälan till nämnden uppgav HS följande. I april 2022 fick hon ett sms som såg ut att komma från banken. I sms:et stod att banken misstänkte bedräglig aktivitet på hennes konto och hon ombads att kontakta spärrservice på ett angivet nummer. Eftersom sms:et låg i samma tråd som tidigare meddelanden från banken var hon säker på att det var från banken. Hon kände inte till fenomenet spoofing.

Under samtalet med det som hon trodde var spärrservice fick hon information om att någon hade kommit över hennes BankID, vilket gjorde henne oerhört stressad och rädd. Kvinnan som hon pratade med rekommenderade henne att endast ha ett BankID och för att säkerställa övergången från det gamla till det nya BankID:t, som hon skulle få hjälp att ladda ned, behövdes ett supportprogram laddas ned till hennes mobil. Hon laddade sedan ned ett nytt BankID från bankens hemsida på sin dator. Kvinnan framstod som mycket professionell. Hon lämnade inte ut några uppgifter om kortnummer, koder eller dylikt under telefonsamtalet.

De obehöriga transaktionerna från hennes konton i banken uppgår till totalt 290 846 kr och fördelar sig på två konton: 119 656 kr från hennes personkonto samt 171 190 kr från hennes plusgirokonto. Hon driver ett aktiebolag och är anställd i företaget. Med det stulna mobila BankID:t har bedragarna genomfört obehöriga transaktioner som hon inte är ansvarig för. Som företrädare för ett mindre bolag så innebär en stöld av företagets pengar att det inte finns pengar att dela ut lön eller betala företagets utgifter med. Hon som privatperson kan bli personligt ansvarig att betala företagets skatter och avgifter om företaget saknar betalningsförmåga. Bedragarna har gjort obehöriga uttag på företagets konto med hjälp av det stulna BankID:t som utfärdats i hennes namn genom ett avtal som hon i egenskap av konsument har med banken. Detta möjliggjordes genom att hon som konsument blev bedragen och lurad, och hennes privata BankID stulet. Nämnden bör därför pröva samtliga transaktioner.

Banken motsatte sig kravet och begärde att nämnden ska avvisa kravet i den del det avser transaktioner som är hänförliga till HS:s näringsverksamhet samt avslå kravet i övrigt.

I sitt svar till nämnden uppgav företaget följande.

Det är HS:s bolag som har ingått avtal med banken om företagskontot, som är ett plusgirokonto. Denna kontotyp erbjuds inte till konsumenter. Transaktionerna om 171 190 kr som är hänförliga till detta konto är inte att bedöma som konsumentrelaterade. Kravet i den delen bör därför avvisas.

Vad gäller ärendet i övrigt gör banken gällande att transaktionerna har kunnat genomföras till följd av att en skyldighet enligt 5 kap. 6 § betaltjänstlagen har åsidosatts genom grov oaktsamhet och att

handlandet dessutom är att anse som särskilt klandervärt i betaltjänstlagens mening. Banken har därför inte någon skyldighet att återställa kontot i detta fall.

BankID är en personlig elektronisk legitimation som kan användas för legitimering (inloggning) till myndigheter och företag med e-tjänster och för underskrift (signering) av avtal eller andra överenskommelser. Syftet är alltså inte begränsat till konsumentrelaterade åtgärder.

Enligt bankens utredning är de transaktioner som är föremål för prövning signerade med BankID. Detta BankID skapades genom att HS först legitimerade sig med sitt mobila BankID och skannade en första QR-kod för att kunna logga in i bankens självserviceportal för BankID. Därefter signerade hon nedladdning av ett nytt mobilt BankID med sitt befintliga mobila BankID. När man signerar nedladdning av ett nytt mobilt BankID framgår det tydligt på skärmen vad signeringen avser. Det varnas även uttryckligen för att aldrig ladda ner ett BankID på uppmaning av vare sig banken eller någon annan person, oavsett orsak. Banken har alltså vid det aktuella tillfället uppmanat HS att inte signera precis den åtgärd som hon ändå valde att signera.

Därefter har HS slutligen möjliggjort för bedragaren att tillse att det nya BankID:t hamnade på bedragarens enhet. HS har laddat ned fjärrstyrningsappen AnyDesk till sin mobil. Genom att ladda ned fjärrstyrningsprogrammet och sedan dela sin skärm, möjliggjorde HS för bedragaren att tillse att det nya BankID:t slutligen hamnade på bedragarens enhet. HS måste ha hållit fram sin telefon mot skärmen så att bedragaren kunde starta kamera-appen och läsa med sin (bedragarens) enhet den sista QR-koden som genererades i självserviceportalen, eller på annat sätt delat QR-koden med bedragaren. Sedan signeringen av nedladdning har skett, slutförs nämligen nedladdningen av ett nytt mobilt BankID till en ny enhet genom att den nya enheten läser den andra QR-kod som genereras på skärmen.

Enligt bankens mening har situationen i detta fall varit sådan att anmälaren måste ha insett att hon var i färd med att bli bedragen. Bland annat ombads hon att installera och använda ett fjärrstyrningsprogram och fick även ta del av ett varningsmeddelande på sin skärm om att aldrig ladda ner ett BankID på uppmaning av vare sig banken eller någon annan person, oavsett orsak. Varningsmeddelandet gav alltså kunden anledning att anta att hon inte var i kontakt med banken eftersom man aldrig ska signera åtgärden ens på uppmaning av (det man uppfattar som) banken. Genom att trots det ändå fullfölja bedragarens instruktioner har anmälaren hanterat sina personliga behörighetsfunktioner och betalningsinstrument på ett så pass oaktsamt sätt att handlandet är såväl grovt oaktsam som särskilt klandervärt i betaltjänstlagens mening.

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

Nämnden prövar endast tvister mellan näringsidkare och konsumenter. Detta villkor är inte uppfyllt när det gäller anmälan i den del som avser transaktionerna på HS:s plusgirokonto, som är ett företagskonto. Nämnden prövar därför inte ärendet i den delen.

När det gäller transaktionerna på personkontot gör nämnden följande bedömning.

Av utredningen framgår att HS fick ett sms, som hamnade i samma tråd som tidigare meddelanden från banken. Av sms:et framgick att banken misstänkte bedräglig aktivitet på hennes konto och hon ombads att kontakta bankens spärrservice på ett angivet telefonnummer. Vidare framgår att HS ringde detta nummer och att hon då pratade med en person som förklarade att någon hade kommit över hennes BankID. Det framgår utöver detta att HS laddade ned ett fjärrstyrningsprogram till sin mobil och signerade nedladdningen av ett nytt BankID, som personen använde för att genomföra de aktuella transaktionerna.

Det står klart att HS inte själv genomförde transaktionerna och att dessa gjordes utan hennes samtycke. Det är vidare utrett att transaktionerna kunde genomföras för att HS signerade nedladdningen av ett nytt BankID och gav tillgång till den QR-kod som visades på hennes skärm. Transaktionerna är alltså obehöriga men kunde genomföras eftersom HS inte skyddade de personliga behörighetsfunktioner som var kopplade till hennes BankID.

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

Nämnden konstaterar att det inte framgår av utredningen hur det sms såg ut som HS fick. Utgångspunkten är därför att detta inte hade en utformning eller ett innehåll som kan anses tala för att

HS insåg att det kunde röra sig om ett bedrägeri. Det förhållandet att meddelandet hamnade i samma tråd som tidigare meddelanden från banken talar i stället för att HS inte förstod att så var fallet.

Det förefaller heller inte särskilt osannolikt att det från HS:s perspektiv framstod som rimligt att hon skulle ladda ned ett fjärrstyrningsprogram för att få hjälp med att ladda ned ett nytt BankID. Enligt vad HS har berättat trodde hon som sagt att någon hade kommit över hennes BankID.

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

Vid en sammantagen bedömning utgör de omständigheter som har kommit fram inte tillräcklig bevisning för att HS var medveten om att hon gav en obehörig person tillgång till sitt BankID eller att hon på någon annan grund insåg att det fanns en risk för obehöriga transaktioner. Slutsatsen blir därför att HS inte ska anses ha agerat särskilt klandervärt.

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

Det är som sagt utrett att HS fick ett varningsmeddelande när hon skulle signera nedladdningen av ett nytt BankID. Enligt nämndens mening får det i allmänhet krävas att man tar del av meddelanden av det slaget, även om man uppfattar förhållandena som pressande. Om HS hade tagit del av meddelandet, som var tydligt och kortfattat, skulle hon ha förstått att det fanns en påtaglig risk för att transaktioner skulle genomföras utan hennes samtycke. Genom att i stället signera nedladdningen av ett nytt BankID har HS på ett mycket tydligt sätt avvikit från den aktsamhet som kan krävas av henne. Hon har således genom grov oaktsamhet försummat skyldigheten att skydda sin personliga behörighetsfunktion.

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

Skiljaktig mening

Två av ledamöterna var skiljaktiga i fråga om motiveringen och anförde följande.

Vi delar majoritetens bedömning att HS genom grov oaktsamhet försummat skyldigheten att skydda sin personliga behörighetsfunktion. Vi anser emellertid inte att det i allmänhet kan krävas att konsumenter tar del av ett varningsmeddelande från BankID oaktat konsumentens upplevelse i form av stress eller press.

I nya och överraskande situationer känner sig konsumenter okunniga och osäkra. Detta i kombination med en upplevelse av tidspress och behov av att agera snabbt gör konsumenter stressade. Osäkra och otydliga situationer upplevs ofta som hotande vilket skapar psykologisk och fysiologisk stress. I situationer som upplevs som osäkra och stressande ökar vidare konsumenters tendenser att se till andra människor för vägledning om hur de bör agera. Konsumenter agerar enligt andras uppmaningar när situationen är osäker, särskilt om konsumenten uppfattar den andre som en auktoritet. För en konsument som försätts i en stressad situation kan därför en bedragares anvisningar framstå som både adekvata och lämpliga även om det i efterhand går att ifrågasätta rimligheten i bedragarens instruktioner. Utöver ovan nämnda allmänna faktorer så finns det ett stort antal individrelaterade faktorer som påverkar förmågan att hantera stressade situationer såsom låg ålder, hög ålder,

personlighet och hög osäkerhetsintolerans. Det ska vidare tilläggas att konsumenter i förhållande till banken är den svagare parten och skyddsvärda och att alltför höga krav således inte kan ställas på konsumenterna. Vi delar därmed inte majoritetens bedömning att konsumenter i allmänhet bör ta del av varningsmeddelanden från BankID även om en situation upplevs som pressande/stressande. Vi anser således inte att det förhållande att HS mottog ett varningsmeddelande har någon avgörande betydelse för bedömningen av hennes agerande. I övrigt delar vi majoritetens motivering och beslut.