Obehöriga transaktioner. En konsument har i samband med ett bedrägeri laddat ner en app som gjort det möjligt för annan att fjärrstyra hans dator samtidigt som han, på bedragarens uppmaning, skapat ett nytt BankID och skannat en QR-kod. Med hjälp av fjärrstyrningen har bedragaren genomfört en transaktion från konsumentens konto. Konsumentens agerande har ansetts grovt oaktsamt (men inte särskilt klandervärt) och han ska därför stå för endast en del av förlusten.

Beslut 2022-11-09; 2022-03828

ASM begärde ersättning med 59 800 kr.

I sin anmälan till nämnden uppgav han följande. Han fick ett sms som såg ut att komma från banken med information om att han behövde beställa ett nytt BankID eftersom banken misstänkte bedräglig aktivitet på hans konto. Han ringde numret som stod i sms:et och kom, som han uppfattade det, till bnkens växel. Kvinnan han pratade med visste att han hade tre BankID och sa att han behövde spärra de två äldsta och därefter skapa ett nytt. Han fick ett nytt sms med en länk för att han skulle ladda ner en app som motsvarade bankens supportprogram. Appen gjorde så att kvinnan kunde fjärrstyra hans skrivbord. Kvinnan bad honom därefter att skapa ett nytt BankID och skanna QR-koden. Därefter genomfördes obehöriga transaktioner till ett belopp om totalt 59 800 kr, varav 29 900 kr från hans privatkonto och 29 900 kr från hans företagskonto. Han ringde till banken och fick då information om att banken inte hade varit inblandad. Eftersom sms:en hamnade i samma tråd som sms från banken bör banken kompensera honom för den bristande säkerheten.

Banken motsatte sig kravet.

I sitt svar till nämnden uppgav banken följande. Av ASM:s egna uppgifter framkommer att han låtit en annan person ta del av hans personliga koder till Mobilt BankID vid i vart fall ett till två tillfällen alternativt vid något av tillfällena hjälpt bedragaren att skapa ett Mobilt BankID som ASM inte har haft tillgång till. Förfarandet strider mot bankens allmänna villkor och att lämna ut sin kod till sitt mobila BankID har av Högsta domstolen i mål nr T 930-21 ansetts innebära att kriterierna för en tillitsfullmakt är uppfyllda och att denna behörighet kan omfatta även andra rättshandlingar än de som huvudmannen har avsett att mottagaren skulle företa. Av samma anledning menar banken att transaktionerna är behörigt utförda.

Banken menar vidare att ASM vid ett flertal tillfällen har haft möjlighet att fundera över förfarandet och i vart fall vid något tillfälle ifrågasätta agerandet. Ett dylikt agerande att – utan ifrågasättande och utan att närmare undersöka förhållandena – i strid med de allmänna villkoren följa en okänd uppringares instruktioner att knappa in samt lämna ut koder och tillåta fjärrstyrning av sin dator kan inte anses vara annat än särskilt klandervärt. Banken ska därför inte behöva svara för någon del av de belopp som frånhänts ASM. I vart fall ska ASM anses ha agerat grovt vårdslöst.

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

Nämnden prövar endast tvister mellan näringsidkare och konsumenter. Detta villkor är inte uppfyllt när det gäller anmälan i den del som avser transaktionen på ASM:s företagskonto. Nämnden prövar därför inte ärendet i den delen. När det gäller transaktionen på hans privatkonto gör nämnden följande bedömning.

Av utredningen i ärendet framgår att ASM fick ett sms som såg ut att komma från banken och att han ringde det nummer som han uppmanades att ringa i sms:et. Det framgår att han förmåddes ladda ner en app som gjorde att kvinnan som han pratade med kunde fjärrstyra hans dator samtidigt som han, på bedragarens uppmaning, skapade ett nytt BankID och skannade en QR-kod. Det får anses utrett att bedragaren, med hjälp av fjärrstyrningen, kunde se den kod som det nya BankID:et genererade och att man därmed kunde genomföra den aktuella transaktionen. Det står alltså klart att ASM inte har skyddat de personliga behörighetsfunktioner som har varit knutna till hans konto och att transaktionen kunde genomföras till följd av denna underlåtenhet.

Det är även utrett att bedragaren genomförde transaktionen utan att ASM hade samtyckt till detta. Det rör sig alltså om en obehörig transaktion. Huruvida bedragaren därmed har kunnat binda ASM i förhållande till tredje man enligt de kriterier som tillämpas för s.k. tillitsfullmakter saknar betydelse i detta sammanhang.

Utredningen visar inte annat än att ASM trodde att han fick hjälp av en företrädare för banken och att han därmed uppfattade att det var en behörig person som fick insyn i hans hantering av BankID. Han har alltså inte avsiktligt avslöjat de personliga behörighetsfunktionerna för en obehörig person.

Det framgår att ASM tillät fjärrstyrningen för att han blev lurad att tro att det pågick ett bedrägeriförsök på hans konto och det får antas att han trodde att hans agerande var nödvändigt för att skydda sina tillgångar. Det har inte kommit fram något som talar för att han då insåg att det fanns en risk för att personen skulle genomföra de transaktioner som kom att ske. Han kan därmed inte anses ha varit likgiltig till risken för obehöriga transaktioner. Slutsatsen blir därför att han inte kan anses ha agerat särskilt klandervärt. Han ansvarar således inte för hela förlusten.

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

Det får normalt anses förenat med tydliga risker att låta någon fjärrstyra en dator samtidigt som man hanterar koder och andra behörighetsfunktioner som man därmed riskerar att avslöja. Därför får det i regel krävas att man ifrågasätter behovet av sådana åtgärder och att man gör vad man kan för att kontrollera vem man ger en sådan insyn. Detta gäller även om man har uppfattat förhållandena som pressande och oavsett om det har saknats särskilda skäl för att ifrågasätta bedragarens uppgifter.

Genom att tillåta fjärrstyrningen och därmed ge någon annan möjlighet att bl.a. ta del av den QR-kod som hans BankID genererade har ASM på ett mycket tydligt sätt avvikit från den aktsamhet som kan krävas av honom. Han har således genom grov oaktsamhet försummat skyldigheten att skydda sin personliga behörighetsfunktion.

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

Skiljaktig mening

Två ledamöter är skiljaktiga och ansåg att anmälan av följande skäl inte ska prövas heller när det gäller transaktionen på ASM:s privatkonto.

ASM har uppgett följande om händelsen.

Han fick ett sms som såg ut att komma från hans bank och det hamnade i samma sms-flöde som tidigare meddelanden från banken. I sms:et stod att banken misstänkte obehörig aktivitet på hans konto och att han behövde beställa ett nytt BankID. Han ringde upp numret som var angivet och kom till en kvinna som sa att han hade tre olika BankID och att de två äldsta behövde spärras. Han behövde också skaffa ett nytt BankID.

Kvinnan skickade ett nytt sms med en länk för att han skulle ladda ner en app som motsvarade bankens supportprogram. Appen gjorde så att kvinnan kunde se hans skrivbord på datorn. Kvinnan bad honom därefter att skapa ett nytt BankID och skanna en QR-kod, vilket han gjorde.

Av bankens svaromål och den tekniska utredning som banken gett in i ärendet framgår att någon har skapat ett nytt Mobilt BankID i ASM:s namn genom användning av ASM:s befintliga Mobila BankID. Det nya Mobila BankID:et har sedan använts för att utföra den omtvistade transaktionen. Det är även visat att banken har skickat ett sms med engångskoder i anslutning till beställningen av Mobilt BankID samt ett sms med information om att ett nytt Mobilt BankID har skapats.

Vilka åtgärder som vidtagits och av vem när det nya Mobila BankID:et skapades är oklart.

ASM har inte lämnat några närmare uppgifter i ärendet om hur det nya Mobila BankID:et skapades. Banken anger i sitt svaromål att ASM har uppgett att han låtit en annan person ta del av hans personliga koder till Mobilt BankID alternativt hjälpt personen att skapa ett Mobilt BankID. ASM har dock inte klargjort vilket av dessa två tillvägagångssätt som är korrekt. ASM har inte heller lämnat någon förklaring till varför han inte kan redogöra för hur det faktiskt gick till.

Vi noterar att ASM har gjort vissa uttalanden som kan uppfattas som att han har lämnat ut koder – svarskoder eller kod till sitt Mobila BankID – under samtalet. Det framgår av en inlaga där ASM kommenterar händelseförloppet i hans eget ärende i ljuset av rättsfallet NJA 2022 s. 522. Det är dock oklart vad ASM gör gällande i detta avseende.

I sammanhanget bör även beaktas att ASM inte har gett in någon dokumentation som visar hur det inledande sms:et såg ut, dvs. där han uppmanades att spärra sitt BankID och ringa ett visst nummer. Han har inte heller nämnt något om den applikation som han laddade ned och som möjliggjorde fjärrstyrningen.

Det är alltså inte utrett vad som ska prövas i ärendet, dvs. om ASM har brustit i skyldigheten att skydda sina personliga behörighetsfunktioner (5 kap. 6 § p. 1 betaltjänstlagen) eller om han underlåtit att följa villkoren som gäller för Mobilt BankID (5 kap. 6 § p. 3 betaltjänstlagen).

Det går alltså inte att avgöra ärendet utifrån befintlig utredning. Mot bakgrund av ärendets karaktär och vad som hittills framkommit i utredningen anser vi inte att det är lämpligt att avgöra ärendet utan att höra parterna. ASM:s talan ska därför avvisas.