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; 2022-01950

BF begärde ersättning med ersättning med i första hand 66 000 kr och i andra hand 51 000 kr.

I sin anmälan till nämnden uppgav han följande. Den 16 juli 2021 fick han ett sms som såg ut att komma från hans bank; det innehöll bl.a. bankens logga och informationen verkade seriös. I sms:et stod att banken misstänkte obehörig aktivitet på hans konto och att han uppmanades kontakta banken snarast på ett angivet telefonnummer. Han ringde upp numret och en person svarade med ”Bankens Spärrservice”. Personen verkade trovärdig och berättade att någon i England försökt komma in på hans konto och att han därför behövde spärra kortet och skaffa ett nytt BankID.

Han loggade in på sin bankdosa och fick siffror som han knappade in. Han lämnade sifforna från dosan till personen han pratade med. Han uppmanades sedan att öppna sitt BankID. Han såg då att det kom upp en ikon med ett nytt BankID. Personen han pratade med sa sedan att de skulle höras efter helgen eftersom det var fredag kväll. Efter att ha pratat med sin dotter ringde han banken för att kontrollera om någon därifrån kontaktat honom. Han fick då information om att uttag om totalt 66 000 kr hade gjorts från hans konton. Han gjorde sedan en polisanmälan och spärrade sitt kort.

Banken har efter händelsen utökat och förtydligat sina varningar för bedrägerier med BankID.

Han begär i första hand att banken betalar tillbaka hela beloppet. I andra hand begär han ersättning med avdrag för en självrisk om 15 000 kr eftersom han var oaktsam med sitt BankID och blev lurad.

Banken motsatte sig kravet.

I sitt svar till nämnden uppgav banken följande. Trots varningstexter om felaktiga sms och uppmaning att aldrig lämna koder till okända personer har BF ringt numret i sms:et utan att kontrollera vem det tillhör. Under samtalet har han vidare, på uppmaning av en okänd person, lämnat ut svarskoder från sin personliga säkerhetsdosa vid två tillfällen. Svarskoderna har använts för att genomföra en inloggning på Internetbanken och för att signera beställning av nytt mobilt BankID. Någon kontroll av vad svarskoderna skulle användas till gjordes inte.

Enligt bankens villkor förbinder sig kunden att inte avslöja kod/lösenord för någon. Av villkoren framgår vidare att banken aldrig efterfrågar uppgifter om kontonummer, CVV-kod, pinkoder eller liknande.

BF har agerat på ett sätt som inte bara varit grovt oaktsamt utan också särskilt klandervärt och bör därmed själv ansvara för det reklamerade beloppet.

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 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 normalt 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 BF 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 under samtalet förmåddes tro att någon hade försökt komma in på hans konto. Under samtalet lurades han att lämna ut svarskoder från sin säkerhetsdosa och därmed kunde man genomföra den aktuella transaktionen. Det står således klart att BF 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 transaktionen utan att BF hade samtyckt till detta. Det rör sig alltså om en obehörig transaktion.

Frågan är härefter om BF:s underlåtenhet att skydda svarskoderna har varit särskilt klandervärd eller grovt oaktsam.

Utredningen visar inte annat än att BF trodde att han lämnade koderna till en företrädare för banken och att denna person var behörig att använda svarskoderna. Han har alltså inte avsiktligt överlämnat svarskoderna till en obehörig person.

Det framgår att BF lämnade ut koderna för att han blev lurad att tro att någon hade försökt komma in på hans konto och det får antas att han trodde att utlämnandet 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 den transaktion 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 BF:s agerande ska bedömas som grovt oaktsamt.

Det får normalt anses förenat med tydliga risker att överlämna koder till någon annan och utan möjlighet att kontrollera hur koderna används eller sprids. Därför får det i regel krävas att man ifrågasätter behovet av att överlämna koder 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. Detta gäller även om man har uppfattat förhållandena som pressande och oavsett om det har saknats särskilda skäl att ifrågasätta bedragarens uppgifter.

Genom att muntligen lämna ut koderna får BF på ett mycket tydligt sätt anses ha avvikit från den aktsamhet som kan krävas av honom. Han har således genom grov oaktsamhet försummat skyldigheten att skydda sin personliga behörighetsfunktion.

BF: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 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 avsiktligen 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 i princip ska 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 behörighets-funktioner 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 BF fick ett sms som såg ut att komma från banken. Sms:et varnade för en obehörig aktivitet på hans konto och uppmanade honom att ta en kontakt med banken på ett visst nummer, vilket han gjorde. Under samtalet informerades han om att han behövde spärra sitt kort och skaffa ett nytt BankID och han lurades att lämna ut svarskoder från sin säkerhetsdosa. Koderna användes sedan för att skapa ett nytt Mobilt BankID i BF:s namn som sedan användes för att genomföra de reklamerade transaktionerna.

Det är utrett att bedragaren genomförde transaktionen utan att BF hade samtyckt till detta. Det rör sig alltså om en obehörig transaktion.

Frågan är härefter om BF:s utlämnande av svarskoder 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. I detta fall har banken även framfört att det i bankens kontovillkor anges att banken aldrig efterfrågar uppgifter om koder.

Varje muntligt utlämnade av personliga behörighetsfunktioner innebär alltså, objektivt sett, ett utlämnade 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 rättsfallet NJA 2022 s. 522.

BF har lämnat en kortfattad redogörelse för samtalet med bedragaren, men utan att beskriva hur han upplevde samtalet och den person han talade med. Han har inte påstått att han gjorde några försök att ta reda på vem han talade med eller att han ställde kontrollfrågor till bedragaren för att ta reda på varför det var nödvändigt att lämna ut svarskoder från bankdosan (jfr t.ex. p. 32-33 i domskälen i rättsfallet NJA 2022 s. 522). Ingenting tyder på att han inte kände till hur bankdosan fungerar och vad koderna används till.

Vad BF har uppgett om utformningen av sms:et, dess innehåll och samtalet med bedragaren tyder på att det var fråga om ett förslaget bedrägeri.

Han borde inte desto mindre ha förstått att det förelåg en risk för obehöriga transaktioner när han lämnade ut koderna till en för honom okänd person. Det kan dock inte anses visat att han avsiktligen lämnade ut koderna till en obehörig person.

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

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

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