Lagen om obehöriga transaktioner med betalningsinstrument. Fråga om kontohavarens ansvar för transaktioner som utförts av bedragare. Kontohavaren blev uppringd av någon som utgav sig för att arbeta på banken (I) och som genom s.k. spoofing föreföll ringa från bankens telefonnummer (II). Kontohavarna har lurats att legitimera sig genom sitt Mobila BankID. Till följd av detta har bedragarna kunnat föra bort pengar.

Beslut 2018-06-14; 2017-07814 (I) och 2017-13660 (II)

I

LH begärde ersättning med 45 000 kr för obehöriga transaktioner.

I sin anmälan till nämnden uppgav LH följande. Hon blev uppringd av en person vid namn Daniel som uppgav att han arbetade på banken. Han förklarade att hennes konto hade blivit kapat och uppmanade henne därför att logga in på sitt Mobila BankID för att spärra kontot och förhindra ytterligare kapningsförsök, vilket hon gjorde två gånger. Hon kontrollringde till banken strax efter samtalet med Daniel och fick då veta att hon blivit utsatt för bedrägeri. – Hon använder inte BankID för att logga in på internetbanken, utan använder det som identifieringsmetod i arbetssammanhang. Hon har inte heller sådana tekniska kunskaper som behövs för att förstå vad appen har för funktioner. I en pressad situation som denna var hennes agerande fullt naturligt. Det är inte någon ursäkt från bankens sida att man har gått ut med information i media och varnat kunder för bedragare. Det är uppenbart att banken har säkerhetsbrister.

Banken motsatte sig kravet.

I sitt svar till nämnden uppgav banken följande. LH tog emot ett telefonsamtal från ett skyddat nummer från en okänd person som sa sig ringa från banken och bad henne att identifiera sig med sitt Mobila BankID. LH gjorde det utan någon som helst kontroll av vem som ringde upp. Därigenom fick den okände personen tillgång till LH:s internetbank. Därefter utförde LH ytterligare en BankID-signering, varvid bedragaren kunde ladda ner ett nytt Mobilt BankID. Bedragaren skapade därefter ett Swish-konto och bytte telefonnummer för att sedan göra överföringarna. – Det har under flera års tid varnats från bankerna, polisen, radio, TV och media i övrigt för att man aldrig på begäran från någon okänd person ska lämna ut sina bankuppgifter eller logga in på sin internetbank. När bankens kunder loggar in på internetbanken får de sådan information i en varningstext. LH:s agerande måste anses så klandervärt att det vore stötande om banken skulle behöva stå för någon del av förlusten. Hon bör därför ansvara för hela beloppet. I vart fall har LH varit grovt vårdslös.

Allmänna reklamationsnämnden, i utökad sammansättning, gjorde följande bedömning.

Är lagen om obehöriga transaktioner med betalningsinstrument tillämplig?

Lagen om obehöriga transaktioner med betalningsinstrument gäller kontohavares ansvar för belopp som belastar ett konto på grund av en obehörig transaktion med ett betalnings-instrument (1 §).

Ett *betalningsinstrument* kan vara ett kontokort eller något annat personligt instrument eller en personlig rutin som används för att elektroniskt initiera en betalningstransaktion (2 § 1). Av lagens förarbeten framgår att ett BankID är ett sådant betalningsinstrument (se prop. 2009/10:122 s. 24). En *obehörig transaktion* är en transaktion som genomförs utan samtycke från kontohavaren eller någon annan som enligt kontoavtalet är behörig att använda betalningsinstrumentet (2 § 2).

Parterna är överens om att LH blev kontaktad av en bedragare som genom användning av Mobilt BankID och Swish lyckades föra över 45 000 kr från hennes konto. Nämnden konstaterar att LH inte godkände Swish-överföringen och alltså inte samtyckte till transaktionen. Det är därför fråga om en obehörig transaktion i lagens mening.

När ansvarar kontohavaren för en obehörig transaktion?

En kontohavare är skyldig att skydda sin personliga kod och vid vetskap om att betalnings-instrumentet kommit bort eller använts obehörigen snarast anmäla detta till betaltjänst-leverantören samt i övrigt följa de villkor som enligt kontoavtalet gäller för användning av betalningsinstrumentet (4 §). Om en obehörig transaktion kunnat genomföras på grund av att kontohavaren genom grov oaktsamhet åsidosatt sina skyldigheter enligt 4 §, ansvarar kontohavaren för beloppet. Om kontohavaren är konsument är ansvaret begränsat till 12 000 kr. Har kontohavaren handlat särskilt klandervärt ansvarar denne dock för hela beloppet (6 §).

Enligt lagens förarbeten tar bestämmelserna om *grov oaktsamhet* sikte på situationer då kontohavaren har varit obetänksam på ett sätt som inte kan ursäktas. Vid bedömningen ska särskild hänsyn tas till arten av de personliga säkerhetsanordningar som hör till ett betalningsinstrument och till de omständigheter under vilka det förlorades, stals eller missbrukades. En samlad bedömning får göras utifrån den miljö och situation kontohavaren befunnit sig i samt hans eller hennes möjlighet att skydda sig mot en obehörig transaktion. Det måste också tas hänsyn till om kontohavaren är en konsument. Personliga omständigheter kan ha betydelse för bedömningen, t.ex. kontohavarens ålder (se prop. 2009/10:122 s. 17 och 27 f.).

Om kontohavaren varit grovt oaktsam, ska ställning tas till om hen kan anses ha handlat *särskilt klandervärt.* Enligt förarbetena kan så vara fallet om kontohavaren har agerat så klandervärt i förhållande till betaltjänstleverantören att det skulle vara stötande att denne behöver stå för någon del av den obehöriga transaktionen. Det ska närmast röra sig om fall där kontohavaren genom sitt handlande får anses ha varit likgiltig till risken för obehöriga transaktioner. Som exempel nämns att kontohavaren – trots villkoren – lämnar ett kontokort

lättillgängligt och obevakat under en lång tid på en badstrand med mycket folk, i ett omklädningsrum eller i en garderob på en restaurang, eller att kontohavaren lämnar ifrån sig kortet på en nattklubb för löpande debiteringar under en lång tid (se prop. 2009/2010:122 s. 29).

Nämnden har i tidigare avgöranden ansett att konsumenter har agerat särskilt klandervärt när de, efter att ha blivit kontaktade på Facebook, har lämnat ut koder från sin bankdosa (ARN 2013-04700) eller har loggat in på sin internetbank med användande av sitt Mobila BankID (ARN 2017-02060).

Avtalsvillkoren

Av bankens allmänna villkor för Mobilt BankID framgår att Mobilt BankID är att betrakta som en värdehandling och därför ska förvaras och hanteras på ett betryggande sätt (p. 4).

I villkoren anges också att innehavaren står risken om någon obehörig använt Mobilt BankID (p. 4) samt att innehavaren ansvarar för alla förpliktelser som uppkommer som en följd av att Mobilt BankID används (p. 6). I det avseendet lägger villkoren alltså ett större ansvar på kontohavaren än vad som anges i lagen om obehöriga transaktioner med betalnings-instrument. Nämnden konstaterar att avtalsvillkor som i jämförelse med bestämmelserna i lagen är till nackdel för en konsument är utan verkan mot honom eller henne (3 §). Nämnda villkor ska därför lämnas utan avseende.

Nämndens bedömning

Det konstateras att en bedragare förmådde kontohavaren LH att använda sitt Mobila BankID till att identifiera sig/signera mot banken två gånger. Därigenom kunde bedragaren logga in på hennes internetbank och skapa ett nytt Mobilt BankID. Bedragaren skapade därefter ett Swish-konto, bytte telefonnummer för Swish och förde över 45 000 kr från LH:s konto via Swish.

Frågan är om LH:s agerande har inneburit att hon varit grovt oaktsam i lagens mening. Nämnden konstaterar att LH identifierade sig mot banken med hjälp av sitt Mobila BankID efter att ha blivit uppringd av en okänd person från ett skyddat telefonnummer. Nämnden anser att LH därmed inte hanterat sitt Mobila BankID på ett betryggande sätt i enlighet med avtalsvillkoren för Mobilt BankID. Nämnden anser, vid en sammantagen bedömning av omständigheterna i ärendet, att LH agerat på ett sätt som varit grovt oaktsamt. Hon ska därför enligt 6 § lagen om obehöriga transaktioner med betalningsinstrument i vart fall ansvara för förlusten till ett belopp om 12 000 kr.

Om LH dessutom ska anses ha agerat särskilt klandervärt ska hon ansvara för hela beloppet. Nämnden konstaterar att LH blev utsatt för ett förslaget bedrägeri. Hon trodde att hon pratade med banken och hon befann sig i en pressad situation. Hon trodde sig inte göra något annat än att identifiera sig mot banken med hjälp av sitt Mobila BankID. Det saknas utredning om vilken information som visades för LH i displayen när hon använde sitt Mobila BankID. Hon lämnade inte ut några koder till bedragaren. Nämnden konstaterar också att det inte finns någon möjlighet för konsumenterna att styra över bankernas säkerhetslösningar. Oavsett

bankens varningar för bedrägerier, står det klart att LH som konsument inte förstod att hennes användning av BankID:t kunde få så långtgående konsekvenser. Nämnden bedömer att LH:s agerande inte har inneburit att hon var likgiltig inför risken för obehöriga transaktioner. Nämnden anser att hon inte heller agerat på något annat sätt som medför att hon ska anses ha varit särskilt klandervärd.

Banken ska därför ersätta LH för det obehöriga uttaget, med avdrag för 12 000 kr.

II

HB begärde ersättning med 140 000 kr för obehöriga transaktioner.

I sin anmälan till nämnden uppgav HB följande. Han blev uppringd från bankens privata kundtjänstnummer. Han kände igen numret eftersom han är kund hos banken. En Johan Andersson presenterade sig och sade att han ringde från banken. Johan pratade svenska och frågade var HB för tillfället befann sig. Han svarade att han var hemma i sin lägenhet i Helsingborg. Johan sade att det i Berlin pågick en transaktion på hans konto. För att kontrollera status på sina konton så loggade han omedelbart in på sin internetbank. Inloggningen gjordes på hans laptop och legitimering skedde via Mobilt BankID. Johan sade att de måste blockera transaktionen och bad honom att legitimera sig via Mobilt BankID. HB sade till Johan att det inte kändes rätt att göra det. Johan var väldigt övertygande och lugn. HB tänkte att han fått ett liknande samtal från banken ungefär tio år tidigare, då hans bankkort hade blivit ”skimmat” och någon tog ut pengar från en bankomat i Peru. Dessutom gick han in på hitta.se och kontrollerade telefonnumret och fick bekräftat att det var bankens nummer. Därför beslutade han sig för att starta den Mobila BankID-appen. Han såg i appen att han var på väg att legitimera sig mot banken. Eftersom han själv redan var inloggad hade han inte en tanke på att han gjorde något annat än att just legitimera sig. Han tryckte in sin kod i Mobila BankID-appen. Johan sade att transaktionen nu kunde stoppas. HB var själv inloggad på sin dator och såg att allt fortfarande verkade normalt. Johan bad honom därefter att legitimera sig igen för att kunna blockera hans Mobila BankID, vilket han då gjorde. Därefter avslutades samtalet. Strax efteråt såg han att någon gjorde en obehörig Swish-transaktion på 5 000 kr från hans personkonto. Han ringde omedelbart till banken på samma nummer som han nyss blivit uppringd ifrån. Han hamnade i telefonkö och medan han satt i kö såg han hur bedragaren flyttade pengar från hans kapitalkonto till hans personkonto där Swish är anslutet. Han förde tillbaka pengarna till kapitalkontot för att förhindra möjligheten att Swisha, men bedragaren flyttade återigen tillbaka pengarna till personkontot. Innan han kom fram till bankens kundtjänst hade fyra Swish-transaktioner på totalt 140 000 kr gjorts från hans personkonto till tre okända personer. – På bankens hemsida, och i den tillfälliga information som banken gått ut med, kan man läsa att en bedragare kan utge sig för att ringa från banken, men det står inget om att en bedragare till och med kan ringa från bankens eget telefonnummer. Det som var avgörande för att HB, efter noga överväganden och diskussion med Johan, startade Mobilt BankID-appen var att Johan ringde från bankens telefonnummer.

HB anser att det är en allvarlig säkerhetsbrist hos banken att någon kan logga in på hans internetbank när han själv redan är inloggad. Bedragarnas inloggning skedde inom några minuter och med största sannolikhet från en helt annan fysisk plats, som han omöjligt hade kunnat förflytta sig till. Banken bör också se över om det ska vara så enkelt att justera beloppsbegränsningen för Swish. Andra banker kräver fler steg med säkerhetsåtgärder.

Banken motsatte sig kravet.

I sitt svar till nämnden uppgav banken följande. HB blev uppringd av en person som presenterade sig som Johan Andersson och som sade att han ringde från banken. Enligt polisanmälan tyckte HB att samtalet lät suspekt men lät sig övertalas. Bedragaren hade vetskap om HB:s personnummer och kunde, genom att HB tryckte sin säkerhetskod, logga in på hans internetbank. Därefter bad bedragaren HB att ytterligare en gång legitimera sig med sitt Mobila BankID. I displayen hos HB framgick då att han godkände ett nytt Mobilt BankID. Med det nya Mobila BankID:t kunde bedragaren därefter göra överföringarna via Swish.

Denna typ av bedrägerier har förekommit i Sverige under relativt lång tid. Det händer att bedragaren "spoofar" ett telefonnummer som då syns i displayen i bankkundens mobiltelefon. Detta kan göras genom att bedragaren laddar ner en app som finns att tillgå på marknaden, vilket banken inte kan göra något åt. Bankerna har under lång tid varnat för denna och andra typer av bedrägerier. Bankerna har också informerat om att en bank aldrig kontaktar kunder och ber dem lämna ut sina koder eller legitimera sig med Mobilt BankID. Banken varnar för detta på första sidan när kunden loggar in på internetbanken. I press, radio och TV förekommer löpande information och varningar.

Enligt bankens villkor för Mobilt BankID framgår att innehavaren ansvarar om någon obehörig använt Mobilt BankID. HB har medverkat till bedrägeriet genom att på uppdrag av en okänd person vid två tillfällen inom ramen för samma händelse logga in på sin internetbank och också godkänna ett nytt Mobilt BankID. Man kan ifrågasätta om förfarandet ska anses innebära att överföringarna alls ska betraktas som obehöriga. Det är i realiteten en fullmakt som HB gett bedragaren. Under alla förhållanden är det Bankens uppfattning att förfarandet sammantaget ska anses vara så obetänksamt att det skulle vara stötande om banken ska stå för något belopp. I vart fall har HB varit grovt vårdslös.

Allmänna reklamationsnämnden, i utökad sammansättning, gjorde följande bedömning.

Är lagen om obehöriga transaktioner med betalningsinstrument tillämplig?

Lagen om obehöriga transaktioner med betalningsinstrument gäller kontohavares ansvar för belopp som belastar ett konto på grund av en obehörig transaktion med ett betalnings-instrument (1 §).

Ett *betalningsinstrument* kan vara ett kontokort eller något annat personligt instrument eller en personlig rutin som används för att elektroniskt initiera en betalningstransaktion (2 § 1). Av lagens förarbeten framgår att ett BankID är ett sådant betalningsinstrument (se prop. 2009/10:122 s. 24). En *obehörig transaktion* är en transaktion som genomförs utan samtycke

från kontohavaren eller någon annan som enligt kontoavtalet är behörig att använda betalningsinstrumentet (2 § 2).

Parterna är överens om att HB blev kontaktad av en bedragare som genom användning av Mobilt BankID och Swish lyckades föra över 140 000 kr från hans konto. Nämnden konstaterar att HB inte godkände Swish-överföringarna och alltså inte samtyckte till transaktionerna. Det är därför fråga om obehöriga transaktioner i lagens mening.

När ansvarar kontohavaren för en obehörig transaktion?

[Som ovan i referat I.]

Avtalsvillkoren

[Som ovan i referat I.]

Nämndens bedömning

Det konstateras att en bedragare förmådde kontohavaren HB att använda sitt Mobila BankID till att identifiera sig/signera mot banken två gånger. Därigenom kunde bedragaren logga in på hans internetbank och skapa ett nytt Mobilt BankID. Bedragaren skapade därefter ett Swish-konto, bytte telefonnummer för Swish och förde över 140 000 kr från HBs konto via Swish.

Frågan är om HB:s agerande har inneburit att han varit grovt oaktsam i lagens mening. Nämnden konstaterar att HB, som visserligen trodde att samtalet kom från bankens telefonnummer, identifierade sig mot banken med hjälp av sitt Mobila BankID efter att ha blivit uppringd av en okänd person. Nämnden anser att HB därmed inte hanterat sitt Mobila BankID på ett betryggande sätt i enlighet med avtalsvillkoren för Mobilt BankID. Nämnden anser, vid en sammantagen bedömning av omständigheterna i ärendet, att HB agerat på ett sätt som varit grovt oaktsamt. Han ska därför enligt 6 § lagen om obehöriga transaktioner med betalningsinstrument i vart fall ansvara för förlusten till ett belopp om 12 000 kr.

Om HB dessutom ska anses ha agerat särskilt klandervärt ska han ansvara för hela beloppet. Nämnden konstaterar att HB har blivit utsatt för ett förslaget bedrägeri. Han blev uppringd från bankens telefonnummer, han trodde att han pratade med banken och han befann sig i en pressad situation. Han trodde sig inte göra något annat än att identifiera sig mot banken med hjälp av sitt Mobila BankID. Det saknas utredning om vilken information som visades för HB i displayen när han använde sitt Mobila BankID. Han lämnade inte ut några koder till bedragaren. Nämnden konstaterar också att det inte finns någon möjlighet för konsumenterna att styra över bankernas säkerhetslösningar. Oavsett bankens varningar för bedrägerier, står det klart att HB som konsument inte förstod att hans användning av BankID:t kunde få så långtgående konsekvenser. Nämnden bedömer att HB:s agerande inte har inneburit att han varit likgiltig inför risken för obehöriga transaktioner. Nämnden anser att han inte heller agerat på något annat sätt som medför att han ska anses ha varit särskilt klandervärd.

Banken ska därför ersätta HB för de obehöriga uttagen, med avdrag för 12 000 kr.