Obehöriga transaktioner. En konsument, som i samband med ett bedrägeri lämnat ut sina kortuppgifter till en okänd person samt använt sitt BankID i enlighet med den okände personens instruktioner, anses ha agerat särskilt klandervärt och ska därför stå för hela förlusten.

Beslut 2022-11-09; 2022-03987

ET begärde ersättning med 72 178 kr.

I sin anmälan till nämnden uppgav hon följande. Hon skulle studera i Umeå och behövde flytta dit med kort varsel och sökte därför boende. Via en bostadgrupp på Facebook kom hon i kontakt med en kvinna som ville hyra ut en lägenhet. Hon kontaktade kvinnan via Messenger och fick bilder på lägenheten, planritning och adress till lägenheten. Tanken var att en visning skulle äga rum på distans, via Messenger eller Facetime. Kvinnan verkade väldigt trovärdig. Kvinnan ville ta en kreditupplysning på henne och senare samma dag var hennes BankID och internetbank spärrade. Hon kontaktade därför banken och fick då veta att två köp om sammanlagt 72 178 kr hade gjorts, ett i Litauen och två i Malta. Hon har inte lämnat ut sina kontouppgifter.

Banken motsatte sig kravet.

I sitt svar till nämnden uppgav banken följande.Transaktionerna initierades genom att kortnumret till ET:s Debit-kort angavs hos ett inköpsställe på internet och därefter godkändes med ett BankID utställt i ET:s namn. Kortuppgifterna framgår inte i internetbanken. Banken kan inte dra någon annan slutsats än att ET har lämnat ut sina kortuppgifter till bedragaren.

En inloggning gjordes på ET:s internetbank den aktuella dagen. Med hjälp av BankID ändrades hennes telefonnummer och därefter gjordes en ansökan om ett nytt BankID. Ansökan om det nya BankID:t gjordes med hjälp av hennes tidigare BankID. De aktuella transaktionerna godkändes med det nyskapade BankID:t.

Dessa skeenden innebär att ET måste ha använt sitt BankID ett flertal gånger på uppmaning av bedragaren. Till banken har ET dessutom uppgett att hon har scannat en QR-kod på uppmaning av bedragaren.

I strid mot kontovillkoren har ET alltså dels lämnat ut sina kortuppgifter, dels gett personen tillgång till hennes internetbank.

Banken anser att agerandet har varit grovt oaktsamt och dessutom särskilt klandervärt. ET har inte befunnit sig i en pressad situation och det har inte framkommit några andra omständigheter som ursäktar hennes agerande. Hon har således varit likgiltig inför risken för obehöriga transaktioner och hon har därmed agerat särskilt klandervärt. Hon är därför betalningsansvarig för transaktionerna utan någon beloppsbegränsning. I vart fall har hon agerat grovt oaktsamt och är därför ansvarig för transaktionerna till ett belopp om 12 000 kr.

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

Av utredningen i ärendet framgår att ET kom i kontakt med en kvinna som ville hyra ut en lägenhet till henne. Det framgår att kvinnan ville ta en kreditupplysning på ET och det får anses utrett att hon på uppmaning av kvinnan skannade en QR-kod som hennes BankID hade genererat. Det framgår vidare att en inloggning ägde rum på ET:s internetbank och att ett nytt BankID togs ut i hennes namn. De aktuella transaktionerna initierades med hjälp av ET:s kortuppgifter och godkändes med hjälp av hennes BankID. Det får även anses utrett att kortuppgifterna inte fanns tillgängliga på internetbanken. Av detta drar nämnden slutsatsen att ET förmåddes lämna ut kortuppgifter och att hon även lurades att godkänna ett antal åtgärder med hjälp av BankID. Det står därmed klart att ET inte har skyddat de personliga behörighetsfunktioner som har varit knutna till hennes konto och att transaktionerna kunde genomföras till följd av denna underlåtenhet.

Det är även klarlagt att bedragaren genomförde transaktionerna utan att ET hade samtyckt till detta. Det rör sig alltså om obehöriga transaktioner.

Frågan är härefter om ET:s underlåtenhet att skydda kortuppgifterna och sitt BankID, och i förlängningen sina personliga behörighetsuppgifter, har varit särskilt klandervärd eller grovt oaktsam.

ET lämnade ut kortuppgifterna till en person som utgav sig för att vilja hyra ut en lägenhet till henne och använde sitt BankID i enlighet med personens instruktioner. Det står därmed klart att hon var medveten om att personen inte var behörig att hantera hennes uppgifter. Det kan visserligen vara så att hon då inte insåg att det fanns en stor sannolikhet för att uppgifterna skulle missbrukas. Att avslöja sina kortuppgifter för en okänd person och använda sitt BankID på det sett som har skett måste

emellertid anses vara förknippat med en påtaglig fara för obehöriga transaktioner. Det måste rimligen krävas att man inser detta.

Slutsatsen blir därför att ET med avsikt har gett en obehörig person tillgång till sina personliga behörighetsfunktioner och att hon samtidigt hade anledning att misstänka att det förelåg en betydande eller närliggande risk för att hennes handlande kunde medföra en förlust. Det förhållandet att hon behövde hyra en lägenhet med kort varsel ursäktar inte hennes agerande. ET har således på ett särskilt klandervärt sätt försummat skyldigheten att skydda sin personliga behörighetsfunktion. Detta innebär att hon svarar för hela förlusten. Hennes krav ska därmed avslås.

Skiljaktiga meningar

Två ledamöter är skiljaktiga i fråga om motiveringen till nämndens beslut och anförde följande.

Av utredningen i ärendet framgår att ET kom i kontakt med en kvinna via Facebook som skulle hyra ut en lägenhet till henne. Kvinnan uppgav via Messenger att hon behövde en kreditupplysning avseende ET inför uthyrningen och skickade en QR-kod till henne för detta ändamål. Av ingivna underlag i ärendet framgår att ET bekräftade olika åtgärder med sitt mobila BankID i sin telefon (”BankID-app”). Först identifierade hon sig mot banken. Efter identifieringen, som gav bedragaren åtkomst till hennes internetbank, ändrade hon det telefonnummer hon sedan tidigare registrerat hos banken till bedragarens telefonnummer. Åtgärden medförde att banken skickade ett sms till henne med texten *”Dina kontaktuppgifter hos oss har ändrats. Var det inte du som ändrade, ring oss och identifiera dig”*. ET använde strax därefter sin BankID-app på nytt, denna gång för att godkänna åtgärden att aktivera ett nytt mobilt BankID. Därefter gjorde bedragaren korttransaktioner från ETs konto genom att uppge ETs kortuppgifter på en e-handelssida samt genom att bekräfta kortköpet med det nyskapade BankID:t.

ET har uppgett att hon inte lämnade ut sina kortuppgifter vid händelsen. Enligt bankens uppgifter fanns inte kortuppgifterna tillgängliga i internetbanken. Det får därför anses utrett att ET lämnade ut sina kortuppgifter till bedragaren.

Ärendet rör inte utlämnande av personliga behörighetsfunktioner utan ET:s hantering av sina betalningsinstrument (kortnummer och mobilt BankID). Frågan är om hon därvid har agerat i strid med skyldigheten att följa de villkor som enligt avtalet gäller för användning av betalningsinstrumentet (5 kap. 6 § p. 3 betaltjänstlagen) och, om så är fallet, om hon på så vis har orsakat de obehöriga transaktionerna genom ett grov oaktsamt eller särskilt klandervärt handlande.

Av kortvillkoren framgår att kortet, varmed även avses kortnumret, ska förvaras och hanteras på ett sådant sätt att ingen annan ges tillfälle att använda det. När det gäller hanteringen av säkerhetslösningar (t ex mobilt BankID) anges i avtalsvillkoren att kunden ska vara vaksam vid användningen av säkerhetslösningen och är skyldig att inte använda säkerhetslösningen på ett sätt som ger någon obehörig tillgång till kundens konton eller tjänster i banken. ET har alltså agerat i strid med gällande avtalsvillkor.

När det gäller bedömningen av hennes handlande konstaterar vi att det inte var fråga om ett förslaget bedrägeri. Redan vid den inledande åtgärden i BankID-appen, dvs. att identifiera sig mot banken, måste ET ha förstått att det inte var fråga om att beställa en kreditupplysning på sig själv från ett kreditupplysningsföretag. När ET sedan bekräftade registreringen av ett nytt

telefonnummer (som inte var hennes eget) hos banken och ansökte om nytt mobilt BankID måste hon under alla förhållanden ha insett att det rörde sig om ett bedrägeri. Det var för övrigt inte någon pressad situation. Åtgärderna gentemot banken gjordes på uppmaning av en för henne okänd privatperson via kontakt på Messenger.

Vid en samlad bedömning av omständigheterna i ärendet anser vi att de obehöriga transaktionerna har kunnat genomföras till följd av att ET har åsidosatt sin skyldighet att följa villkoren för betalningsinstrumentet på ett särskilt klandervärt sätt. Hennes yrkande ska därför avslås.

Två ledamöter är skiljaktiga i fråga om nämndens bedömning och anförde följande.

Det står klart att ET förmåtts att godkänna skapandet av ett nytt BankID och att lämna ut kortuppgifter till en bedragare. Hon har därmed inte skyddat de personliga behörighetsfunktioner som varit knutna till hennes konto, vilket lett till att de aktuella transaktionerna har kunnat genomföras. Frågan är därmed om ET genom grov oaktsamhet har åsidosatt sin skyldighet att skydda de personliga behörighetsfunktionerna.

Det får normalt anses förenat med tydliga risker att överlämna kortuppgifter till någon annan samt att godkänna skapandet av ett nytt BankID utan möjlighet att kontrollera hur uppgifterna används eller sprids. Det får därför i regel krävas att man ifrågasätter behovet av att överlämna uppgifter på det sätt som har skett och att man gör vad man kan för att kontrollera vem man överlämnar kortuppgifterna 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 lämna ut kortuppgifterna och godkänna skapandet av ett nytt BankID får ET anses ha avvikit från den aktsamhet som rimligen kan krävas av henne. Hon har således genom grov oaktsamhet försummat skyldigheten att skydda sina personliga behörighetsfunktioner.

Frågan är härefter om ET har agerat särskilt klandervärt.

Utredningen visar inte annat än att ET trodde att hon lämnade kortuppgifterna till en person i syfte att personen skulle kunna ta en kreditupplysning på henne inför en lägenhetsuthyrning. Av utredningen framgår även att hon av samma anledning lurades att godkänna skapandet av ett nytt BankID. Banken Bank har inte bevisat att hon avsiktligen överlämnade kortuppgifter till en obehörig person eller avsiktligen godkände skapandet av ett nytt BankID. Banken har inte heller visat att hon insåg att det fanns en risk för att personen skulle genomföra de transaktioner som kom att ske. Det är därmed inte styrkt att hon har varit likgiltig till risken för obehöriga transaktioner. Slutsatsen blir därför att hon inte kan anses ha agerat särskilt klandervärt. Hon ansvarar således inte för hela förlusten utan hennes 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 henne.