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 och lämnade under samtalet ut svarskoder från sin bankdosa. Till följd av detta har bedragarna kunnat föra bort pengar (I-II).

Beslut 2018-06-14; 2017-10285 (I) och 2017-12130 (II)

I

IJ begärde ersättning med 150 107 kr för obehöriga transaktioner.

I sin anmälan till nämnden uppgav IJ följande. Medan hennes make var inlagd på sjukhus blev hon uppringd av en man som uppgav att han hette Jan Axelsson och arbetade på bankens säkerhetsavdelning. Axelsson förklarade att han nyss hade talat med hennes make som hade uppmanat honom att kontakta henne. Makens konto hade nämligen blivit utsatt för kapnings-försök och bankkortet behövde spärras omedelbart i syfte att förhindra ytterligare uttags-försök. Eftersom maken inte hade tillgång till internetbanken behövde hon vara behjälplig med att spärra kortet. Axelsson bad henne ta fram sin bankdosa och gav henne en kod att slå in, vilket hon gjorde. Därefter slog hon in sin pinkod för att få fram en svarskod som hon sedan uppgav för Axelsson. Eftersom det var problem med internetanslutningen bad Axelsson henne att göra om detta några gånger. När hon kontrollerade kontot strax efter samtalet upptäckte hon att det hade skett sammanlagt fyra överföringar om totalt nästan 200 000 kr. Hon ringde genast bankens säkerhetsavdelning för att anmäla detta. Vid samtalet med banken blev hon informerad om att dessa typer av bedrägerier var vanliga och att betalnings-mottagaren var välkänd för att slussa över stora summor pengar, ofta härrörande från brottslig verksamhet, till okända mottagare i utlandet.

Banken har inte informerat om riskerna att bli utsatt för brott. Om den här typen av bedrägeri är ett välkänt fenomen borde banken ändra sina säkerhetsrutiner.

Banken motsatte sig kravet.

I sitt svar till nämnden uppgav banken följande. Fyra överföringar om 46 239 kr, 56 049 kr, 78 009 kr respektive 16 049 kr gjordes från IJ:s konto, varav banken har betalat tillbaka 46 239 kr. I första hand ska transaktionerna inte bedömas som obehöriga, eftersom de inte hade kunnat ske utan IJ:s aktiva medverkan. Transaktionerna är genomförda på ett korrekt sätt. I andra hand ska IJ:s agerande bedömas som särskilt klandervärt och i tredje hand grovt oaktsamt. Hennes handlande är så aningslöst att det skulle vara stötande om banken skulle stå för någon del av det begärda beloppet. Samtliga transaktioner har gjorts med kortläsare utan sladd, vilket innebär att IJ:s pinkod angavs vid genomförande av varje enskild transaktion. Hon har, utan någon egentlig kontroll av Axelssons uppgifter, lämnat ut svarskoder fyra gånger och därigenom gett Axelsson tillgång till sin internetbank. Enligt de allmänna villkoren är inloggningsrutinen personlig och får endast användas av kunden. Banken

kontaktar under inga omständigheter sina kunder med begäran om utlämnande av inloggningsuppgifter och en sådan begäran skulle dessutom stå i strid med villkoren för bankens internettjänst. IJ hade kunnat motringa banken och kontrollera Axelssons uppgifter.

Det finns inga brister i bankens säkerhetsrutiner. På bankens hemsida finns information om vad kunden själv kan göra ur ett säkerhetsperspektiv. Där anges bl.a. att kunden inte ska lämna ifrån sig uppgifter om inloggningskort, pinkod och de svarskoder som genereras när kunden använder sin kortläsare med kort.

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 betalningsinstrument (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 en bankdosa som möjliggör transaktioner via Internet 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).

Banken har hävdat att transaktionerna borde bedömas som behöriga, eftersom de inte hade kunnat ske utan IJ:s aktiva medverkan. Nämnden konstaterar dock att det avgörande är om transaktionerna har skett med eller utan samtycke från kontohavaren.

Parterna är överens om att IJ har blivit kontaktad av bedragare som, genom att lura henne att lämna ut svarskoderna från sin bankdosa, har lyckats föra över 150 107 kr från hennes konto. IJ har inte samtyckt till transaktionerna. Det är därför fråga om obehöriga transaktioner i lagens mening.

När ansvarar kontohavaren för en obehörig transaktion?

En kontohavare är skyldig att skydda sin personliga kod och vid vetskap om att betalningsinstrumentet kommit bort eller använts obehörigen snarast anmäla detta till betaltjänstleverantören 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 internettjänsten framgår att Betalningsinstrument är personligt instrument eller rutin, t.ex. personliga koder, som används av kunden för att initiera en betalningstransaktion (p. 2). Inloggningsrutinerna är personliga och får endast användas av kunden. Kunden får inte låta någon annan använda Inloggningsrutinerna, Internettjänsten eller Telefontjänsterna (p. 5). För att skydda den elektroniska identiteten är det mycket viktigt att kunden håller en personlig kod hemlig. Kunden förbinder sig att inte avslöja en personlig kod för någon annan (p. 9).

Nämndens bedömning

Det konstateras att en bedragare förmådde kontohavaren IJ att använda sin bankdosa och lämna ut svarskoden från bankdosan till bedragaren fyra gånger. Därigenom fick bedragaren tillgång till IJ:s internetbank och kunde föra över 150 107 kr från hennes konto.

Frågan är om IJ:s agerande har inneburit att hon varit grovt oaktsam i lagens mening. Nämnden konstaterar att IJ lämnade ut svarskoder från sin bankdosa efter att ha blivit uppringd av en okänd person. IJ lämnade därmed sin personliga kod till en annan person i strid med avtalsvillkoren för internettjänsten. Nämnden anser att IJ agerade 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 IJ dessutom ska anses ha agerat särskilt klandervärt ska hon ansvara för hela beloppet. Nämnden konstaterar att IJ utsattes 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

spärra sin makes bankkort. Nämnden konstaterar att det inte finns någon möjlighet för konsumenterna att styra över bankernas säkerhetslösningar. Oavsett bankens varningar för bedrägerier, står det klart att IJ som konsument inte förstod att hennes användning av bankdosan och utlämnandet av koderna kunde få så långtgående konsekvenser. Mycket talar ändå för att hennes agerande ska anses särskilt klandervärt eftersom hon under samtalet, i strid med villkoren och lagen, fyra gånger lämnade ut sin personliga svarskod från bankdosan till bedragaren. Nämnden konstaterar dock att bedragaren hade mycket specifik kunskap om IJ:s situation, bland annat om att hennes make låg på sjukhus. Hänsyn bör även tas till IJ:s ålder – hon var vid tillfället över 80 år gammal. Nämnden anser vid en sammantagen bedömning av omständigheterna att IJ genom sitt handlande inte har varit likgiltig inför risken för obehöriga transaktioner. Hennes agerande kan inte anses ha varit särskilt klandervärt. 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 IJ för det obehöriga uttaget, med avdrag för 12 000 kr.

Skiljaktig mening

En av nämndens ledamöter var skiljaktig i fråga om IJ ska anses ha handlat särskilt klandervärt och anförde följande. Av utredningen framgår att IJ under telefonsamtalet i strid med villkoren och lagen fyra gånger har lämnat ut personliga svarskoder från bankdosan till en okänd person som ringde till henne. IJ har själv inte tagit initiativ till telefonsamtalet och hon har inte heller kontrollerat identiteten på personen, till exempel genom att motringa. Vidare har hon inte heller haft någon kontroll över vad svarskoderna användes till.

Enligt IJ blev hon uppmanad av personen som ringde att använda sin internetdosa för att spärra sin makes kort. Att IJ vid telefonsamtal från banken skulle behöva identifiera sig för att på bankens initiativ spärra sin makes kort framstår som så märkligt att IJ borde ha reagerat och ifrågasatt uppgifterna.

Mot denna bakgrund ursäktar enligt min mening inte den situation som IJ befann sig i eller hennes ålder hennes agerande och det skulle vara stötande om banken skulle behöva stå för någon del av beloppet som hon har förlorat genom sitt handlande. Hennes agerande framstår som särskilt klandervärt och IJ borde därför själv ska svara för de obehöriga transaktionerna.

II

MF begärde ersättning med 120 000 kr för obehöriga transaktioner.

I sin anmälan till nämnden uppgav MF följande. Banken eller en bluffmakare ringde upp honom från bankens telefonnummer och sade att något såg konstigt ut på hans konto. Han

försökte då logga in och samtidigt kapades hans Mobila BankID och betedde sig underligt. Han lämnade inte ut några uppgifter och han signerade inte heller någonting med sin mobil. Han ringde till bankens kundtjänst och spärrade sitt Mobila BankID samt sina konton. Då hade redan någon ändrat beloppsgräns i Swish, bytt avsändarnumret i Swish, fört över pengar från hans sparkonto till hans lönekonto och sedan obehörigt Swishat 120 000 kr till en okänd mottagare.

Banken har tydligen en eller flera säkerhetsluckor i sina internetsystem. Om någon eller några tagit sig in och kunnat utföra bankaktiviteter, utan att ha tillgång till hans fysiska bankdosa eller hans fysiska telefon där hans Mobila BankID är installerat, måste det vara bankens skyddssystem som brister och inte han som kund.

Banken motsatte sig kravet.

I sitt svar till nämnden uppgav banken följande. Banken har efter utredning konstaterat att MF:s personliga säkerhetsdosa användes vid upprepade tillfällen för att genomföra Swish-betalningen med hjälp av Mobilt BankID. MF har hela tiden haft säkerhetsdosan i sitt förvar.

Säkerhetsdosor som används av banken är unika och personliga. För att kunna genomföra en inloggning eller signering med dosa behöver man ha fysisk tillgång till den kundunika dosan, ange den fyrsiffriga pinkod som valts av kunden för att starta dosan och i dosan mata in en unik åttasiffrig utmaningskod som, under en begränsad tid, gäller för den transaktion eller inloggning som ska signeras. Man måste även inom en begränsad tid mot bankens system korrekt ange den åttasiffriga svarskod (som visas i dosans display) som dosan räknat fram baserat på erhållen utmaningskod. Om ytterligare/efterföljande signering eller inloggning ska genomföras med dosan måste dosans fyrsiffriga pinkod anges på nytt inför varje användning.

För att kunna beställa ett Mobilt BankID krävs en inloggning till internetbanken samt en signering av beställningen. Signeringen utförs med kundens personliga säkerhetsdosa.

Installation och aktivering av Swish sker i ett antal steg och förutsätter att man har ett Mobilt BankID. Byte av Swish-nummer sker genom att man loggar in på sin internetbank, tar bort den befintliga kopplingen till ett mobiltelefonnummer och kopplar ett nytt mobiltelefonnummer till kontot. En engångskod skickas via SMS till det mobiltelefonnummer man har angivit. Denna kod ska sedan anges på internetbanken. Swish-appen aktiveras sedan genom att man anger sitt mobiltelefonnummer i appen och därefter signerar kopplingen med sitt Mobila BankID. Signering av Swish-betalningar sker med Mobilt BankID som tillhör kunden.

MF blev uppringd av någon som sade sig ringa från banken. Under samtalet var händelse-förloppet under en och samma inloggning följande. Klockan 19:18 användes MF:s dosa för att genomföra en inloggning. Klockan 19:20 användes hans dosa för att signera beställning av ett nytt Mobilt BankID. Klockan 19:22 avslutades MF:s befintliga Swish-anslutning och klockan 19:26 skapades en ny Swish-anslutning. Klockan 19:28 användes MF:s dosa för att signera en höjning av beloppsgräns för Swish. För dessa moment har dosan låsts upp med MF:s fyrsiffriga pinkod. Den åttasiffriga utmaningskoden från bankens system har matats in i

dosan, och en åttasiffrig svarskod från dosan har korrekt angivits mot bankens system. Klockan 19:29 aktiverades Swish-applikationen med det Mobila BankID som beställdes under internetsessionen. Klockan 19:30 överfördes 120 000 kr mellan MF:s egna konton. Överföringar mellan egna konton kräver inloggning, men ingen signering eftersom inga pengar lämnar kundens konton i banken. Klockan 19:30 genomfördes en Swish-transaktion av 120 000 kr. Transaktionen genomfördes via den nya Swish-anslutning som skapades under internetsessionen. Swish-transaktionen signerades med det Mobila BankID som beställdes under sessionen. Att koder från MF:s personliga säkerhetsdosa genererats och lämnats av MF själv framgår av spårbarhetsloggarna.

Kundens aktiva medverkan genom inloggning med säkerhetsdosa och med personlig kod krävs för att ett nytt BankID ska kunna beställas, en ny Swish-koppling registreras och beloppsgränserna ändras. Av bankens avtalsvillkor framgår att säkerhetsdosan är personlig och att koder inte får avslöjas. Efter genomförda transaktioner kontaktade MF bankens kundtjänst. Under detta samtal, som finns inspelat, uppgav han: ”… jag håller på med bankdosan här, en massa koder med den här killen…”. Den reklamerade transaktionen om 120 000 kr kunde ske genom att MF vid ett flertal tillfällen lämnade ut koder med hjälp av sin personliga säkerhetsdosa och möjliggjorde för bedragaren att logga in sig på MF:s internetbank, signera beställning av ett nytt BankID och signera höjning av beloppsgräns för Swish. Med hjälp av det nya BankID:et kunde bedragaren signera Swish-betalning till en av bedragaren angiven mottagare.

Eftersom transaktionerna har skett genom inloggning och signering med MF:s personliga säkerhetsdosa bedömer banken transaktionerna som behöriga. Skulle nämnden anse att den reklamerade transaktionen är obehörig, har MF varken följt skyldigheten att skydda personlig kod enligt 4 § lagen om obehöriga transaktioner eller följt bankens villkor för internetbank och användning av säkerhetsdosa. Genom att vid upprepade tillfällen lämna ut koder till en okänd med hjälp av sin säkerhetsdosa har MF enligt bankens mening agerat särskilt klandervärt och bör därmed själv ansvara för det reklamerade beloppet.

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 betalningsinstrument (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 både en bankdosa som möjliggör transaktioner via Internet och ett BankID är sådana 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).

Banken har hävdat att transaktionen borde bedömas som behörig, eftersom den skett med MF:s personliga säkerhetsdosa. Nämnden konstaterar dock att det inte är tillräckligt att kontohavarens säkerhetsdosa har använts för att transaktionen ska anses behörig, utan det krävs dessutom att transaktionen har skett med kontohavarens samtycke.

Parterna är överens om att MF blev kontaktad av bedragare som genom användning av Mobilt BankID och Swish lyckades föra över 120 000 kr från hans konto. MF har inte samtyckt 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 betalningsinstrumentet kommit bort eller använts obehörigen snarast anmäla detta till betaltjänstleverantören 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).

Enligt förarbetena till lagen är det i princip betaltjänstleverantören, dvs. banken, som ska bevisa att kontohavaren har brutit mot en förpliktelse som följer av lagen eller avtalet och om detta skett genom grov oaktsamhet eller handlandet varit särskilt klandervärt. Samtidigt kan det ställas vissa krav på kontohavaren att bidra till utredningen, t.ex. genom att ange var och när betalningsinstrumentet senast användes. I praktiken får kontohavarens uppgifter många gånger läggas till grund för bedömningen. Beroende på omständigheterna kan kontohavaren dock behöva redovisa något som ger stöd åt hans eller hennes uppgifter (se prop. 2009/10:122 s. 27 f.).

Avtalsvillkoren

Av bankens Allmänna villkor för Internet- och telefontjänst privat framgår att kunden inte får avslöja koden till säkerhetsdosan för någon (p. 11).

Nämndens bedömning

Det konstateras att MF blev utsatt för ett bedrägeri. Han har uppgett att han inte lämnade ut några uppgifter till bedragaren, men nämnden anser att banken genom sin utredning och genom den ljudfil som getts in har bevisat att bedragaren förmådde MF att använda sin bankdosa och att lämna uppgift om svarskoden från bankdosan minst tre gånger. Därigenom fick bedragaren tillgång till MF:s internetbank, varvid ett nytt Mobilt BankID skapades och ett nytt telefonnummer kopplades till Swish. Med hjälp av detta kunde bedragaren föra över 120 000 kr från MF:s konto.

Frågan är om MF:s agerande har inneburit att han varit grovt oaktsam i lagens mening. Nämnden konstaterar att MF lämnade ut svarskoder från sin bankdosa efter att ha blivit uppringd av en okänd person. MF lämnade därmed sin personliga kod till en annan person i strid med avtalsvillkoren för internettjänsten. Nämnden anser att MF agerade 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 MF dessutom ska anses ha agerat särskilt klandervärt ska han ansvara för hela beloppet. Nämnden konstaterar att det inte finns någon möjlighet för konsumenterna att styra över bankernas säkerhetslösningar. Oavsett bankens varningar för bedrägerier, kan det ha varit svårt för MF som konsument att inse hur långtgående konsekvenser hans användning av bankdosan och utlämnandet av koderna kunde få. Mycket talar ändå för att hans agerande ska anses särskilt klandervärt eftersom han, i strid mot avtalsvillkoren och lagen, under samtalet lämnade ut sin personliga svarskod från bankdosan till en okänd person vid upprepade tillfällen. Några omständigheter som skulle kunna ursäkta agerandet har inte framkommit. Nämnden anser vid en sammantagen bedömning av omständigheterna att MF:s agerande har varit särskilt klandervärt och att han får anses ha varit likgiltig inför risken för obehöriga transaktioner. Hans krav ska därför avslås.