En konsument fick ett sms med information om att hon behövde genomföra en säkerhetsuppdatering av sitt bank-id. Meddelandet kom i samma tråd som tidigare sms från banken och det innehöll en länk som hon uppmanades att klicka på för att genomföra uppdateringen. Konsumenten knappade in två svarskoder på den webbplats som hon dirigerades till. Det visade sig att länken var falsk och att en bedragare genom förfarandet fick tillgång till koderna och kunde genomföra obehöriga transaktioner från hennes konto.

Nämnden kom fram till att konsumentens agerande varken var grovt oaktsamt eller särskilt klandervärt. Nämnden rekommenderade därför banken att ersätta förlusten med avdrag för den lagstadgade självrisken om 400 kr.

Beslut 2022-12-15; **2021-16194**

MBW begärde ersättning med 90 150 kr.

I sin anmälan till nämnden uppgav MBW följande. Hennes bank-id höll på att gå ut. Den 26 augusti 2021 fick hon ett meddelande med en länk i samma tråd som tidigare sms från banken om att hon behövde uppdatera sitt bank-id på grund av en säkerhetsuppdatering. Det visade sig att länken var falsk och möjliggjorde att bedragare fick tag på koden till hennes bank-id. Den 1 september samma år upptäckte hon att det fattades pengar på tre av hennes konton.

Hon begär ersättning för de obehöriga transaktionerna.

Banken motsatte sig kravet.

I sitt svar till nämnden uppgav banken följande. Bankens tekniska utredning visar att MBW har använt sin bankdosa och lämnat ut två svarskoder. Dessa svarskoder användes för legitimering hos banken, och nedladdning av ett nytt mobilt bank-id. Det var med detta nya bank-id som transaktionerna sedan genomfördes. Banken arbetar med att upplysa och informera kunderna om potentiella risker och aktuella bedrägeriförsök som banken fått kännedom om. För detta har banken bland annat upprättat en särskild sida på bankens webbplats.

Det var inte fråga om en pressad situation i och med att MBW inte blev kontaktad via ett telefonsamtal, utan hon fick ett SMS. Inte heller fanns det några påståenden som skulle medföra ett behov av akuta åtgärder från MBW:s sida. Hon hade således möjlighet att undersöka om det var banken som var den genuina avsändaren, och på så sätt förhindra att säkerhetslösningen användes obehörigen eller ens skapades, exempelvis genom att besöka bankens hemsida eller ringa till bankens kundtjänst.

Banken anser att MBW har agerat på ett sätt som inte bara varit grovt oaktsamt utan även särskilt klandervärt i betaltjänstlagens mening. Under dessa förhållanden har banken ingen ersättningsskyldighet.

Allmänna reklamationsnämnden gjorde följande bedömning.

Rättsliga utgångspunkter

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. Men om transaktionen har kunnat genomföras för att kontohavaren har agerat särskilt klandervärt eller grovt oaktsamt, ska kontohavaren ansvara för hela eller delar av förlusten. För hela förlusten ska kontohavaren ansvara om agerandet anses vara särskilt klandervärt medan ansvaret är begränsat till 12 000 kr i fall av grov oaktsamhet under förutsättning att kontohavaren 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.

För att kontohavarens agerande ska bedömas som särskilt klandervärt krävs i princip att han eller hon har varit likgiltig till risken för obehöriga transaktioner. Det kan t.ex. röra sig om fall där kontohavaren faktiskt insett att det fanns en risk för en obehörig transaktion men ändå har låtit bli att skydda sin kod. Vid denna bedömning får det särskild betydelse till vem kontohavaren uppfattade att den personliga behörighetsfunktionen lämnades ut. Agerandet får i regel anses särskilt klandervärt även 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. (Se rättsfallet NJA 2022 s. 522 ”BankID-bedrägeriet”.)

I fall där kontohavaren inte har varit likgiltig till risken för de obehöriga transaktionerna kan agerandet i allmänhet inte bedömas som särskilt klandervärt. Men om det kan anses att kontohavaren i stället har haft anledning att räkna med risken för en obehörig transaktion, kan agerandet bedömas som grovt oaktsamt. 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. Grovt oaktsamt ska agerandet anses vara om det utgör ett markant avsteg från den aktsamhet som kan krävas. (Se nämndens beslut den 9 november 2022 i ärende nr 2021-12666, 2021-19593, 2022-01950, 2022-02184, 2022-03987 och 2022-03828.)

Nämndens bedömning

Av utredningen i ärendet framgår att MBW fick ett sms som såg ut att komma från banken och att hon klickade på en länk i sms:et för att uppdatera sitt bank-id. Hon lurades att knappa in svarskoder från sin säkerhetsdosa vilket medförde att de aktuella transaktionerna kunde genomföras. Det står således klart att MBW inte har skyddat de personliga behörighetsfunktioner som har varit knutna till hennes säkerhetsdosa och att transaktionerna kunde genomföras till följd av denna underlåtenhet.

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

Nämnden prövar härefter frågan om MBW:s underlåtenhet att skydda svars-koderna ska bedömas som grovt oaktsamt.

MBW har inte lämnat ut några koder muntligt utan endast knappat in dessa på en hemsida som hon dirigerats till efter att ha klickat på länken i ett sms som såg ut att komma från banken. Det har inte framkommit något som talar för att vare sig sms:et eller hemsidan var utformade på ett sätt som borde ha fått henne att misstänka att länken hade skickats av någon annan än banken.

Nämnden bedömer att agerandet inte innebär en sådan avvikelse från normal aktsamhet att det är att anse som grovt oaktsamt. Detta innebär att MBW:s ansvar är begränsat till 400 kr. Med avdrag för detta belopp ska banken därför rekommenderas att ersätta den förlust som de obehöriga transaktionerna har orsakat henne.