**Reklamera obehöriga transaktioner på bankkonto**

När du som bankkund reklamerar obehöriga transaktioner på ett bankkonto till din bank eller vänder dig med en anmälan till Allmänna Reklamationsnämnden, kan denna malltext användas som ett tillägg till reklamationen.

Malltexten är således inte någon tillräcklig reklamationstext, utan är bara avsedd att användas som ett tillägg till en reklamationstext eller som ett tillägg till en anmälan till Allmänna Reklamationsnämnden.

I och med att det är en malltext, är meningen att du ska/kan göra ändringar, så att texten kommer att passa ditt eget fall. Du kan ju som kund till exempel vilja göra gällande att särskild hänsyn ska tas till förmildrande omständigheter, som hög ålder.

**Bankens ansvar för den tekniska säkerheten**

Enligt punkt 32 i skälen till Europaparlamentets och rådets direktiv 2007/64/EG samt punkt 71 i skälen till Europaparlamentets och rådets direktiv (EU) 2015/2366, som betaltjänstlagen till stor del baseras på, bör inte direktiven påverka betaltjänstleverantörens (bankens) ansvar för den tekniska säkerheten. Så som framgår av punkt 91 i skälen till det senare direktivet, är betaltjänstleverantören ansvarig för säkerhetsåtgärderna. Detta går i linje med vad som sägs i proposition 2009/10:122 s. 35.

*”Kontohavaren skall inte kunna bli betalningsansvarig för obehöriga transaktioner som genomförs efter det att kortet eller koden spärranmälts. Detsamma skall gälla när transaktionerna kunnat genomföras på grund av säkerhetsmässiga brister eller något annat fel som utfärdaren av kortet ansvarar för, eller om en näringsidkare har godtagit ett kontokort trots att han eller hon insåg eller borde ha insett att kortet användes utan kontohavarens samtycke.”*

På sidan 34 i samma proposition framgår även följande.

*”Kontohavarens hantering av den till ett kontokort hörande koden utgör en viktig del av systemsäkerheten.”*

Så som framgår av vad som ovan har anförts, kan ansvaret för en obehörig transaktion inte bedömas enkom utifrån kontohavarens hantering av den del av säkerhetslösningen, som kontohavaren har satts att ta hand om. Det måste göras en helhetsbedömning, där en bedömning görs av bankens säkerhetslösningar och i vad mån dessa har inverkat på den uppkomna förlusten.

 **Fredrik Ljunggrens rapport ”Säkerhet vid elektronisk legitimering och underskrift”**

Villaägarnas Riksförbunds chefsjurist Ulf Stenberg har uppdragit till IT-säkerhetsexperten Fredrik Ljunggren på Kirei att närmare utreda säkerhetsproblemen och även få klarlagt vilka åtgärder, som kan vidtas för att öka säkerheten och därmed minska bedrägerierna vid elektronisk legitimering. Detta pga. att många småhusägare och andra konsumenter har drabbats av bedrägerier i samband med elektronisk legitimering och underskrift. Uppdraget har resulterat i Fredrik Ljunggrens rapport ”Säkerhet vid elektronisk legitimering och underskrift”, se bilaga.

Fredrik Ljunggren är en av Sveriges ledande experter på IT-säkerhet. Han deltar bl.a. som säkerhetsexpert i e-legitimationsnämndens granskningsgrupp, som granskar och följer upp säkerheten bland samtliga utfärdare av Svensk e-legitimation. Fredrik Ljunggren är även teknisk expert i ICANNs Registry Services Technical Evaluation Panel (RSTEP) som arbetar med utvärdering av säkerhet och robusthet i det globala domännamnssystemet. Han konsulteras likaså vid brottsutredningar med att säkra bevis eller att avge sakkunnigutlåtande. Han biträder även som expert i IT-rättsliga frågor.

 **Bankens avsaknad av rimlighetsspärrar och manuella kontroller möjliggör obehöriga transaktioner**

Enligt Fredrik Ljunggren håller bankernas säkerhetsdosor och BankID tillräcklig teknisk säkerhet, även om det finns vissa tillkortakommanden, jfr sidan 27 f i anförda rapport. Säkerheten brister dock inte när det gäller säkerhetsdosorna eller BankID utan säkerhetsbristerna avser istället så som framgår på sidan 28 följande.

*”Några säkerhetstekniker som möjliggör identifiering på distans och som inte i någon del beror på viss aktsamhet från den enskildes sida är i dagsläget inte kända. Inte heller traditionella tillvägagångssätt erbjuder absolut säkerhet. Det finns dock en skillnad mellan automatiserad masshantering och personliga besök på till exempel ett bankkontor. En person som kommer in på ett bankkontor med avvikande beteende och som önskar genomföra en rad riskfyllda transaktioner kommer att nekas, eller i vart fall utsättas för särskilt ingående extra kontroller för att kompensera en ökad risk. När motsvarande riskfyllda beteende äger rum med ett BankID fungerar emellertid det automatiserade tillvägagångssättet på samma sätt som vid en transaktion som inte präglas av särskilda risker. Rimlighetsspärrar för särskilt riskfyllda transaktioner och ovanliga användningsmönster måste dock enligt min mening även finnas på plats vid den automatiserade behandlingen. Om en sådan rimlighetsspärr löser ut kan det komma att krävas att en tjänsteman gör en manuell granskning och utför eventuella tillkommande kontroller av diverse slag, innan denna tar beslut om att den ifrågavarande transaktionen ska genomföras. Införandet av sådana rimlighetskontroller ankommer således på tillhandahållaren av tjänsten (t.ex. internetbanken), då det endast är denna som har tillgång till de uppgifter som krävs för kontrollen.*

*Det är därför enligt min mening inte rimligt att ålägga den enskilde ett obegränsat ansvar för obehöriga transaktioner med BankID eller bankdosa.”*

Slutsatsen är således att om banken inte har infört tillräckliga rimlighetsspärrar i sitt system, som i sin tur ska utlösa manuell kontroll och granskning, är det inte rimligt att ålägga den enskilde ett obegränsat ansvar för den obehöriga transaktionen.

På sidan 32 i rapporten framgår vad som är ett avvikande användningsmönster för ett bankkonto.

*”Att med stöd av en helt nyutfärdad e-legitimation länsa sparkontot med överföringar till ett flertal nya och annars okända mottagare är helt enkelt inte ett rimligt användningsmönster.”*

På sidan 23 i rapporten konstateras följande beträffande situationen med ständigt återkommande bankbedrägerier.

*”Med hjälp av svarskoder från bankdosan har bedragarna kunnat erhålla ett BankID, och kan med hjälp av detta genomföra ett stort antal överföringar till andra konton. Det är också med detta nyutfärdade BankID möjligt att hinna plundra konton som innehavaren har i andra banker innan kontohavaren förstår vad som är i görningen och hinner spärra e-legitimationen. Denna form av bedrägerier har förekommit i systematisk form i över ett decennium. Bedragarna har på senare tid dock blivit alltmer slipade och pålästa kring offret och offrets privatliv. Problemen har därvid tilltagit under 2017 och 2018.”*

 **Banken har orsakat de obehöriga transaktionerna på mitt bankkonto**

Bankbedrägerierna har pågått i över ett decennium. Bankerna har förvisso infört olika yttre säkerhetslösningar, som bankdosor och BankID, som ska göra det svårare att logga in på internetbanken för den som är obehörig. När väl bedragaren har tagit sig in på bankkontot, saknas dock inre säkerhetslösningar i form av rimlighetsspärrar för särskilt riskfyllda transaktioner och ovanliga användningsmönster, vilka vid misstänkta transaktioner borde utlösa manuell granskning av tjänsteman för att släppas igenom. I och med att bankerna inte har gjort något åt den inre säkerheten, trots att de sedan mer än ett decennium är medvetna om och har kunnat konstatera säkerhetsbristerna, är det fullkomligt orimligt att bankkunderna ska behöva stå ett obegränsat ansvar för obehöriga transaktioner, som bankerna har haft möjlighet att upptäcka.

Det är istället frågan om ett kalkylerat risktagande från bankens sida, där banken av smidighetsskäl har valt att inte införa en bättre inre säkerhet, allt för att det ska gå lätt att genomföra transaktioner. I och med att dessa förluster till stor del har kunnat föras över på kunderna, minskar detta naturligtvis bankens incitament att göra något åt saken.

Banken har i mitt fall närmast varit likgiltig inför risken för obehöriga transaktioner och får därmed anses ha orsakat eller åtminstone ha varit synnerligen medvållande till de uppkomna förlusterna. Detta då, bedragarens försök till obehöriga transaktioner, när denne lyckats ta sig in på mitt bankkonto, borde ha kunnat fångats upp av rimlighetsspärrar för särskilt riskfyllda transaktioner och ovanliga användningsmönster, vilka sedan kräver manuell granskning av tjänsteman för att släppas igenom.

När det gäller de obehöriga transaktionerna på mitt bankkonto, talar nedanstående för att banken ska stå för dessa.

(I) Ett stort antal obehöriga överföringar gjordes (II) inom loppet av några timmar från det att bedragaren lät utfärda det nya BankID:et och nya Swish. (III) Det är välbekant för banken att risken för obehöriga överföringar är högre vid nyutfärdade BankID och nya Swish-kopplingar. (IV) Likaså när ett flertal överföringar på högre belopp, precis som i mitt fall, (V) sker till ett stort antal personer. (I mitt fall rör det sig om X personer) som jag inte tidigare har gjort överföringar till. (VI) De sammantagna transaktionerna på mitt bankkonto för betalningar räkningar m.m. under de timmar som bedrägeriet pågick uppgår till XXXXXX kr, vilket är mer än de sammanlagda insättningarna och uttagen på ifrågavarande bankkonto under tidsperioden XX-XX-XX. (VII) Bedragarens tillvägagångssätt och handlingsmönster stämmer väl överens med hur bedragare sedan mer än ett decennium tillbaka snabbt tömmer bankkonton, vilket (VIII) är välkänt för banken. (IX) Säkerhetssystemet på banken reagerade ytterst långsamt. Reaktion kom inte förrän efter mer än XX timmar, men då hade bedragaren redan lyckats ta ut stora belopp på kontot. (X) Den sena reaktionen från säkerhetssystemet på banken, visar att banken har avstått från att vidta skadebegränsande åtgärder. Detta gör att en bedragare inte stoppas från att genomföra obehöriga överföringar, när denne väl har lyckats ta sig in på en bankkunds bankkonto. Några rimlighetskontroller larmade inte om det onormala överföringsmönstret på mitt bankkonto, så att någon banktjänsteman hade kunnat stoppa överföringarna. Slutsatsen kan inte bli annat än att när en bedragare väl har tagit sig in på ens bankkonto, låter banken bedragaren vidta i stort sett vilka åtgärder som helst med behållningen på bankkontot.

Bankens säkerhetsmässiga brister har därför möjliggjort för bedragaren att genomföra de obehöriga transaktionerna, varför banken ska svara för de obehöriga transaktionerna på mitt bankkonto. I sammanhanget ska även hänsyn tas till följande förmildrande omständigheter vid bedrägeriet, nämligen att XXXXXX