

Skimningsutrustning

Rättsliga frågor

RättsPM 2011:3 (ersätter RättsPM 2005:22)
Rättsavdelningen
Utvecklingscentrum Stockholm
Mars 2011



ÅKLAGARMYNDIGHETEN

Innehållsförteckning

1. Inledning	3
2. Vad är skimning?	3
3. NJA 2007 s. 774	3
4. NJA 2009 s. 111	4
5. Slutsatser – rättslig bedömning	5

1. Inledning

Denna promemoria beskriver rättsläget i mål då skinningsutrustning har hanterats. Slutsatserna bygger på tolkningen av två rättsfall från Högsta domstolen, NJA 2007 s. 774 och NJA 2009 s. 111.

Syftet med denna promemoria är att ge åklagarna rättslig vägledning i mål där skinningsutrustning förekommer och därigenom uppnå enhetlighet i rättstillämpningen.

Utvecklingscentrum Stockholm redovisade i RättsPM 2005:22 en sammanställning över dåvarande praxis. Genom nu aktuell promemoria upphävs RättsPM 2005:22.

2. Vad är skimming?

En skimmer är en teknisk anordning av varierande storlek som läser av den information som finns lagrad på magnetremsan på ett kredit/konto/betalkort. Skimmern kan monteras på t.ex. uttagsautomater eller handhas av en gärningsman som fått ett kort med magnetremsa i sin besittning och på så sätt har möjligheten att orättmätigt dra kortet genom skimmern. På det sättet kan en kopiering av kortinformationen ske utan att målsäganden känner till att kortet kopierats. Med ett sådant skimmat kort finns stora möjligheter för gärningsmannen att belasta målsägandes konto med obehöriga köp eller uttag innan kortet spärras.

När kortets magnetremsa kopieras genom skimming är det spår nummer två som kopieras. Magnetremsan består av tre spår med information men det är tillräckligt med den information som finns på spår två för att kunna tillverka ett falskt kort. På spår två finns information om vilken bank som givit ut kortet, efternamn och förnamn på den person som kortet tillhör, giltighetstiden för kortet i form av månad och år samt om kortet är försett med chip eller inte. Det bör observeras att den s.k. cvv- eller cvc-koden, d.v.s. den tresiffriga koden på kortets baksida som ofta krävs vid köp via Internet, inte kopieras när ett kort skimmas. Detta innebär att den information som erhålls när ett kort skimmas ofta inte är tillräcklig för att kunna genomföra köp via Internet i Sverige. Det bör dock påpekas att det är upp till försäljaren på Internet att kräva information om denna tresiffriga kod vid ett Internetköp. I Sverige krävs detta i de flesta fall men utomlands är säkerheten inte alltid lika hög. Det är alltså möjligt att genomföra ett köp via Internet med de uppgifter som erhålls när ett kort skimmas under förutsättning att försäljaren på Internet inte kräver information om den tresiffriga koden.¹

3. NJA 2007 s. 774

Högsta domstolen ogillade i detta mål ett åtal angående förberedelse till grovt bedrägeri. Den tilltalade hade beställt en front till en kortläsare och en knapp-sats, vilka varit avsedda att fästas över den fasta utrustningen på en

¹ Uppgifterna bygger på information från kriminalinspektören Christian Söderström vid Rikskriminalen, Finanspolisen

uttagsautomat. Med hjälp av den beställda elektroniska utrustningen skulle såväl automatkundernas pinkod som informationen på magnetremsorna till deras kort läsas av och kopieras. Därefter var det tänkt att "falska" kort skulle tillverkas som skulle användas för uttag i automater eller vid inköp.

Högsta domstolen uttalade att som åtalet var utformat förutsattes för bifall till detta att kortläsaren och knappsatsen varit särskilt ägnade att användas som hjälpmedel för de bedrägerier som brottsplanen syftat till. Enligt domstolen hade kortläsaren och knappsatsen inte varit avsedda att användas vid de bedrägerier som brottsplanen avsett utan endast för att inhämta den information och framställa de kort med vars hjälp bedrägerierna därefter skulle genomföras. Det förelåg därför, enligt Högsta domstolen, inte förutsättningar för att döma den tilltalade för förberedelse till grovt bedrägeri.

Högsta domstolen uttalade vidare att det emellertid kunde hävdas att gärningsbeskrivningen lämnade utrymme för att i stället bedöma gärningen som förberedelse till urkundsförfalskning. En förutsättning för en sådan bedömning angavs dock vara att de kort som var avsedda att framställas med hjälp av informationen från den elektroniska utrustningen på kortläsaren skulle vara att anse som en urkund i den mening som avses i bestämmelsen om urkundsförfalskning i 14 kap. 1 § brottsbalken (BrB). Enligt Högsta domstolen saknades det i målet anledning att ta ställning till denna fråga eftersom försändelsen med kortläsaren och knappsatsen inte kommit den tilltalade tillhanda och han därför inte hade tagit någon sådan befattning med dessa föremål som krävs för att ansvar för förberedelse ska kunna aktualiseras.

4. NJA 2009 s. 111

I detta mål prövade Högsta domstolen ett åtal angående bl.a. grov urkundsförfalskning. Den tilltalade hade tillverkat falska kreditkort genom att förse magnetremsorna på plastkorten med koder som kunde utläsas i kortläsare och som gav sken av att korten var utfärdade av ett bensinbolag och kopplade till olika personers konton i bolaget. Kortet användes sedan i parkeringsautomater. Frågan i målet var om de tillverkade korten utgjorde sådana urkunder som avses i 14 kap. 1 § BrB.

Högsta domstolen uttalade att ett sedvanligt kredit- eller betalkort är en handling som har upprättats till bevis och i övrigt uppfyller de krav som ställs på en urkund enligt 14 kap. 1 § BrB. Det som skilde de kort den tilltalade tillverkat från sedvanliga kreditkort var att de inte var försedda med någon text eller annat som angav vem som var utställare och vem som var innehavare av kreditkortet. Dessa uppgifter framgick i stället av den kod som den tilltalade försett kortens magnetremsor med. Enligt Högsta domstolen gav koden därmed kortet dess specifika innehåll, nämligen att vara ett kreditkort som gav sken av att härröra från bensinbolaget. Den omständigheten att det krävs en maskinell behandling i en kortläsare för att identifiera den skenbara utställaren liksom den kontoinnehavare vars konto skulle belastas fråntog inte korten deras egenskap av att vara urkunder som har upprättats till bevis. Enligt Högsta domstolen var de förfalskade kreditkortet därför sådana urkunder som avses i 14 kap. 1 § BrB. Högsta domstolen förklarade att det åtalade förfarandet var att bedöma som urkundsförfalskning.

Högsta domstolens prövning avsåg endast frågan om förfarandet uppfyllde rekvisiten i bestämmelsen om urkundsförfalskning och frågan om brottet var att bedöma som grovt berördes alltså inte av domstolen.

Hovrätten bedömde däremot frågan om brottets rubricering och uttalade att de aktuella korten endast kunnat användas i parkeringsautomater och att de därmed inte till sin art var sådana att de var särskilt betydelsefulla i den allmänna omsättningen. Men hänsyn till kortens begränsade användningsområde fann hovrätten, trots att det i målet framställt ett förhållandevis stort antal kort, att brottet inte skulle bedömas som grovt.

5. Slutsatser – rättslig bedömning

Av Högsta domstolens uttalanden i NJA 2007 s. 774 framgår att befattning med skimmingsutrustning, som varit avsedd att användas för att inhämta information och framställa kort med vilkas hjälp bedrägerier ska begås, inte kan ligga till grund för ansvar för förberedelse till bedrägeribrott. Högsta domstolen uttalade vidare att en sådan befattning skulle kunna vara att bedöma som förberedelse till urkundsförfalskning. En förutsättning för en sådan bedömning är att de kort som är avsedda att framställas med hjälp av informationen från den elektroniska utrustningen på kortläsaren är att anse som urkunder i den mening som avses i bestämmelsen om urkundsförfalskning i 14 kap. 1 § BrB.

Högsta domstolen har senare i NJA 2009 s. 111 funnit att falska kreditkort som tillverkats genom att magnetremsorna på plastkorten förses med koder som kan utläsas i kortläsare och som ger sken av att korten är utfärdade av ett visst bolag och kopplade till olika personers konton i bolaget är att anse som urkunder i den mening som avses i 14 kap. 1 § BrB.

Mot bakgrund av bl.a. dessa avgöranden kan följande sägas om rättsläget.

Inledningsvis bör nämnas att för att straffrättsligt ansvar över huvud taget ska komma i fråga krävs att den misstänkte tagit befattning med skimmingsutrustningen på något av de sätt som anges i 23 kap. 2 § 1 st. 2 BrB. Att köpa eller sälja, beställa eller utbjuda ett hjälpmedel, t.ex. skimmingsutrustning, utan att någonsin ha innehaft hjälpmedlet utgör inte sådan befattning. Inte heller är det straffbelagt såsom förberedelse att försöka anskaffa hjälpmedel eller att planera sådan anskaffning.²

I det följande ges ett antal exempel på olika typsituationer som kan uppkomma. Det bör observeras att uppräkningsen inte är uttömmande utan endast utgör exempel på situationer som kan förekomma.

- *Förfalskade kort har tillverkats och använts*

I de fall den misstänkte har tillverkat falska kort som även har använts bör förfarandet bedömas som grovt bedrägeri och grov urkundsförfalskning. Användandet av falska kort är en omständighet som kvalificerar

² Wennberg m.fl., Brottsbalken, kommentaren på Internet till 23 kap. 2 § under rubriken "Förberedelsehandlingen"

bedrägeribrottet som grovt, liksom att gärningen varit ägnad att rubba allmänhetens förtroende för bankkort som betalningsmedel.

Urkundsförfalskningen bör bedömas som grov då urkunderna är särskilt betydelsefulla i den allmänna omsättningen. Vidare bör gärningen kunna anses vara av särskilt farlig art bl.a. med hänsyn till att det ofta tillverkats ett stort antal förfalskade kort som använts för omfattande oriktiga uttag eller betalningar från de drabbade kontoinnehavarnas konton, efter att någon olovligen har berett sig tillgång till uppgifter avsedda för automatiserad behandling.

- *Förfalskade kort har tillverkats men ännu ej använts*

Om kort har tillverkats aktualiseras ansvar för förberedelse till grovt bedrägeri. Korten får därvid anses vara särskilt ägnade att användas som hjälpmedel vid bedrägeribrott. Det planerade användandet av falska kort är en omständighet som kvalificerar brottet som grovt liksom den omständigheten att gärningen varit ägnad att rubba allmänhetens förtroende för bankkort som betalningsmedel.

Om den person som misstänks för de tilltänkta bedrägeribrotten också har tillverkat korten torde åtalet avse förberedelse till grovt bedrägeri och grov urkundsförfalskning. Förfalskningsbrottet bör bedömas som grovt då urkunderna är särskilt betydelsefulla i den allmänna omsättningen. Vidare bör, som nämnts ovan, gärningen kunna anses vara av särskilt farlig art bl.a. med hänsyn till att det ofta tillverkats ett stort antal förfalskade kort som varit avsedda att användas för omfattande oriktiga uttag eller betalningar från de drabbade kontoinnehavarnas konton, efter att någon olovligen har berett sig tillgång till uppgifter avsedda för automatiserad behandling.

Om den misstänkte inte har tillverkat korten utan endast tagit annan befattning med dessa, t.ex. förvarat dem, kan ansvar för förberedelse till grovt bedrägeri och förberedelse till brukande av falsk urkund aktualiseras.

- *Inga förfalskade kort har tillverkats men befattning med skimningsutrustning har skett*

I de fall den misstänkte avsett att tillverka falska kredit-/konto-/betalkort men ännu inte gjort detta utan endast på annat sätt befattat sig med skimningsutrustning bör förfarandet vara att bedöma som förberedelse till grov urkundsförfalskning. Knappsatser, filmningsutrustning och liknande föremål får anses vara särskilt ägnade att användas som hjälpmedel vid förfalskningsbrott. Brotten bör ofta vara att anse som grova. Gärningarna bör kunna anses vara av särskilt farlig art med hänsyn bl.a. till att brottsplanen går ut på att, efter att olovligen ha berett sig tillgång till uppgifter avsedda för automatiserad behandling, tillverka ett stort antal förfalskade kort som ska användas för omfattande oriktiga uttag eller betalningar från de drabbade kortinnehavarnas konton. Vidare bör kredit-/konto-/betalkort anses som urkunder som är särskilt betydelsefulla i den allmänna omsättningen.

- *Dataintrång m.m.*

Vid skimming av kort får gärningsmannen anses olovligen bereda sig tillgång till uppgifter som är avsedda för automatisk behandling. I de hittills nämnda situationerna kan därför gärningsbeskrivningarna utformas på ett sådant sätt att de även omfattar dataintrång eller förberedelse till sådant brott. Skimmingen

utgör en nödvändig förutsättning för att kunna framställa falska kort, i de fall detta är avsikten. Dataintrånget kan därför sägas utgöra ett led i förfalskningsbrottet. Vid förberedelse till grov urkundsförfalskning bör, som tidigare nämnts, ett fullbordat eller planerat dataintrång, kunna utgöra en omständighet som kvalificerar brottet som grovt. Om dataintrånget fullbordats bör kunna åtalas för förberedelse till grov urkundsförfalskning medelst dataintrång.

Hovrätten för Västra Sverige har i en dom bedömt hantering av skinningsutrustning som bl.a. dataintrång och förberedelse därtill. Åtalet i målet avsåg i första hand ansvar för förberedelse till grovt bedrägeri. Enligt åtalet hade skinningsutrustning monterats in i en bensinautomat och på flera butikers kortläsare, vilka varit kopplade till kassasystemen. Hovrätten bedömde gärningarna som dataintrång (4 kap. 9 c § BrB), förberedelse till dataintrång och medhjälp till båda dessa brott. Enligt hovrätten hade de tilltalade olovligen berett sig tillgång till uppgifter avsedda för automatiserad behandling. I de fall gärningarna avsåg anskaffande av komponenter för byggande av skinningsutrustning dömdes för förberedelse till dataintrång. Komponenterna ansågs ha varit särskilt ägnade att användas som hjälpmedel vid dataintrång (dom den 8 september 2010 i mål B 3310-10).

- *Informationen från magnetremsan ska användas vid köp på Internet utan att förfalskade kort ska tillverkas*

Rättsläget får betecknas som oklart i de fall det är utrett att avsikten inte har varit att tillverka några falska kort utan att använda informationen från magnetremsan för att beställa varor på Internet. Om den misstänkte ännu inte kommit över information från någon magnetremsa utan endast hanterat skinningsutrustning bör åtalet avse förberedelse till dataintrång. I de fall den misstänkte kommit över information från magnetremsor men ännu inte hunnit använda den bör åtalet avse förberedelse till grovt bedrägeri medelst dataintrång, eftersom dataintrånget kan sägas utgöra ett led i bedrägeribrottet. Bedrägeribrottet bör bedömas som grovt då gärningen varit ägnad att rubba allmänhetens förtroende för bankkort som betalningsmedel. Det bör kunna hävdas att den misstänkte i dessa fall tagit sådan befattning med något – d.v.s. informationen från magnetremsor – som är särskilt ägnat att användas som hjälpmedel vid ett brott. I vart fall föreligger i dessa fall ett fullbordat dataintrång.