Institutionen för Informatik
Handelshögskolan i Göteborg
Göteborgs Universitet

TEKNISKA LÖSNINGAR FÖR BEKÄMPNING AV KONTOKORTSBEDRÄGERIER – Ur e-handlares perspektiv

Magisteruppsats i informatik, 20 p
VT-2002
Handledare: Agneta Ranerup

Författare:
Liv Bryngelsson
Anna Segerstad

Sammanfattning

År 2001 uppgick kontokortsbedrägerier på Internet till 9 miljarder USD, vilket gör det till ett allvarligt ekonomiskt problem för e-handlare.Uppsatsen behandlar området kontokortsbedrägerier inom elektronisk handel och fokus ligger på e-handlarnas perspektiv. Ett syfte är att beskriva hur e-handeln ser ut och fungerar idag, hur kontokortsrelaterade bedrägerier drabbar e-handlarna, de olika aktörerna inom e-handeln och deras beroendeställningar till varandra. Ett annat syfte är att, med hjälp av egenutvecklade modeller, analysera och presentera tekniska lösningar för bedrägeri-bekämpning, samt ge exempel på hur helhetslösningar för förebyggande av kortbedrägerier kan se ut. Huvudaktörerna är e-handlare, systemutvecklingsföretag, kontokortsföretag och kortutfärdare. Det finns beroendeförhållanden mellan aktörerna som påverkar vilka bedrägeribekämpande tekniker som e-handlarna använder. De tekniker som redovisas är; databaser, 'scoring'-verktyg, 'Address Verification System', verifieringskoderna CVV2, CVC2 och CID, samt 'Payer Authentication'-teknikerna Verified by Visa, Secure Payment Authentication och Private Payments. Användningen av de här teknikerna exemplifieras genom redovisningen av tre systemutvecklingsföretags lösningar för bedrägeribekämpning.

E-handlare måste bedriva krig på alla fronter för att ha en chans att överleva. En front är bedragarna, en annan är kontokortsföretagen och kortutfärdarna som man är så starkt beroende av. Det bästa för e-handlarna vore om de fick bestämma själva över vilka bedrägeribekämpande tekniker som de vill ska ingå i deras e-handelslösningar. I stort sett skulle man kunna säga att den perfekta tekniska lösningen för en e-handlare skulle innebära följande; e-handlaren inför tekniken om och när denne själv vill, tekniken lägger inte till något moment för kunden och att kortutfärdaren får stå för kostnaden för 'chargeback', om en transaktion visar sig vara ett bedrägeri. Någon sådan teknik finns inte för närvarande. I dagsläget, anser vi att 'Payer Authentication'-teknikerna är den bästa lösningen som finns för kontokort med magnetremsa.

Förord

Ett stort tack till vår handledare Agneta Ranerup, på Institutionen för Informatik, för all hjälp och vägledning. Vi vill också tacka Freddy Tengberg, som har fungerat som branschkunnig person och bollplank för våra idéer och funderingar. Sist men inte minst vill vi tacka Magnus Bryngelsson, Sven Andersson och Niklas Kjellander, som granskat vår uppsats och gett oss konstruktiv kritik.

Göteborg 23 maj 2002

Anna och Liv

1 Inledning

1.1 Bakgrund

Den här uppsatsen behandlar området kontokortsbedrägerier inom elektronisk handel och fokus ligger på företagens, det vill säga e-handlarnas, perspektiv. Meningen är att, med hjälp av egenutvecklade modeller, analysera och presentera tekniker för bedrägeribekämpning. Teknikerna kommer att presenteras individuellt samt hur de används i en helhetslösning. Idén till ämnet uppkom under en föreläsning på kursen Elektronisk handel, vårterminen 2001, på Systemvetarprogrammet vid Handelshögskolan i Göteborg. Föreläsningen hölls av Freddy Tengberg, VD för e-handelsföretaget Buyonet.

Det har varit turbulens inom e-handeln från dess start. Internet har expanderat i oerhörd fart vilket skapat ett virtuellt Vilda Västern. Samma brott som plågar den verkliga världen frodas i Internets anonymitet. Bedrägerierna på Internet omfattar höga belopp. Kostnaden för bedrägeriförlusterna för alla Internetbetalningar 2001 har beräknats till 9 miljarder USD enligt Meridien Research.[1] Internet-transaktioner utgjorde år 1999 två procent av kontokortsföretaget VISAs samtliga transaktioner. Detta innebär Internettransaktioner för ett värde av 1,48 biljoner USD (1 480 000 000 000 USD).[2] 1999 meddelade VISA International att hälften av VISAs samtliga kontokortsbedrägerier utgörs av Internettransaktioner.[3] Enligt statistik över bedrägerier med VISA- och MasterCardkort i USA så har dock bedrägerierna minskat procentuellt sett.[4] [5] Detta kan tolkas som tecken på att aktörerna inom e-handeln identifierat en del av problemet och arbetar aktivt med att bekämpa Internetbedrägerier. Trots det är Internetbedrägerierna stora, rent ekonomiskt sett, och det gäller att hela tiden ligga steget före bedragarna för att hålla bedrägerierna nere.

Hittills har stor uppmärksamhet inom media riktats mot riskerna som e-handelskunder utsätts för vid e-handel. E-handlarnas utsatta situation, till exempel vid kontokortsbedrägerier, nämns sällan.[6] Enligt Klemow (1999) har e-handlarna ett större behov av bedrägeriförebyggande åtgärder än kunderna. E-handlarna har inget skydd om en kund hävdar att ett köp ej genomförts eller att varan inte levererats.[7] Ett köp där kortinnehavaren har med sig sitt kort och godkänner köpet med sin underskrift kallas för en 'card present'-transaktion. Den bank eller finansiella institution som utfärdat kontokortet står då för kostnaden om transaktionen visar sig vara ett bedrägeri. I fortsättningen kommer de här aktörerna att benämnas kortutfärdare. Vid en transaktion över Internet, en så kallad 'card not present'-transaktion, saknas en fysisk signatur. Det är då e-handlaren som får stå för kostnaden om en sådan transaktion visar sig vara bedrägeri och resulterar i en s.k. 'chargeback'.[8] [9] Eftersom betalning med kontokort är det vanligaste sättet att betala över Internet[10] [11] är e-handlarna

[1] Linda Punch, *Building an Online Fortress* (Credit Card Management, 2001).
[2] Patricia A. Murphy, *The murky world of 'Net chargebacks* (Credit Card Management, New York, 2000), 12, 11, s. 54–60.
[3] Orla O'Sullivan, *Egg on its visage* (USBanker, New York, 1999), 109, 6, s. 22.
[4] *Online Banking Statistics – Statistics for General and Online Card Fraud.* (ePayment Resource Center, 2001).
[5] Ibid.
[6] Marcia Savage, *Online Fraud: New Twist on Old Issue* (Computer Reseller News, 2000), 887, s. 28.
[7] Jason Klemow, *Credit Card Transactions via the Internet* (TMA Journal, Atlanta, 1999), 19, 1, s. 10–14.
[8] Marcia Savage, *Online Fraud: New Twist on Old Issue* (Computer Reseller News, Manhasset, 2000), 887, s. 28.
[9] 'Chargeback' är den tekniska termen som används för att beskriva återbetalningsprocessen när ett kort har använts felaktigt. Processen är mellan kortutfärdaren och handlarens bank. Ett exempel är om en kund nekar till ett köp. Då återförs köpbeloppet till kundens konto och e-handlaren debiteras köpbeloppet samt en avgift för administration. 'Chargebacks' presenteras mer utförligt i avsnitt 3.5.
[10] Kaye Caldwell, *The Public Policy Report* (CommerceNet Newsletter, maj 2001), 3, nr. 5.
[11] David Whiteley, *e-Commerce, Strategy, Technologies and Applications* (The McGraw-Hill Publishing Company, London, 2000).

beroende av kontokortsföretag som till exempel VISA och MasterCard. Kontokortsföretagen arbetar bland annat med bedrägeribekämpande tekniker. E-handlare kan, genom exempelvis hot om högre avgifter eller böter, tvingas att investera i kontokortsföretagens bedrägeribekämpande tekniker. En e-handlare som inte följer VISAs regelverk och normer kan drabbas av böter från 50 000 USD och uppåt.[12]

Det finns fler aktörer än kontokortsföretag, kortutfärdare och e-handlare inom branschen. En aktör inom branschen är systemutvecklingsföretagen som utvecklar bedrägeriförebyggande system åt e-handlarna. De här fyra aktörerna är uppsatsens huvudaktörer. Övriga aktörer som beskrivs är branschorganisationer, e-handlarnas kunder och försäkringsbolag. Branschorganisationerna består ofta av en sammanslutning av flera aktörer som jobbar tillsammans för att begränsa bedrägerier. I vissa fall kan statliga organ vara medlemmar i de här organisationerna. Försäkringsbolagen är en relativt ny aktör i detta sammanhang. Deras försäkringar kan hjälpa e-handlare som blir utsatta för stora bedrägerier.

För att komma till rätta med kontokortsbedrägerierna arbetar e-handlarna, kortutfärdarna och kontokortsföretagen med olika lösningar. Majoriteten av dem är tekniska lösningar men man försöker även, genom exempelvis branschorganisationerna, bearbeta problemet genom att dela erfarenheter och data. Många av de tekniska lösningarna är effektiva mot bedrägerier men någonstans måste man hitta en balansgång mellan vad kunder, e-handlare och kortutfärdare är villiga att investera i, använda och uppdatera.[13]

1.2 Syfte och frågeställningar

Ett mål med uppsatsen är att den ska ge läsaren en förståelse för e-handlarnas situation, dels i kampen mot bedrägerier, dels deras beroendeställning till de mäktiga kontokortsföretagen. Aktörerna inom e-handel har skilda vägar till samma mål, nämligen ekonomisk framgång. Genom att förstå deras situation blir det intressant att titta på vilka tekniker som är framtagna av de olika aktörerna och varför de använder dem. Följande punkter sammanfattar uppsatsens huvudsyften:

- ge en översikt över hur e-handeln ser ut och fungerar idag.
- ge en översikt över kontokortsrelaterade bedrägerier inom e-handel, beskriva vidden av problemet samt hur bedrägerierna drabbar e-handlarna.
- beskriva de olika aktörerna inom e-handeln och deras beroendeställningar till varandra, med hjälp av egenutvecklade modeller.
- analysera och presentera några tekniska lösningar; hur de är uppbyggda och hur de påverkar e-handlarens situation, med hjälp av två modeller som är utvecklade för detta ändamål.
- ge exempel på hur systemutvecklingsföretags helhetslösningar för förebyggande av kortbedrägerier kan se ut.

[12] Linda Punch, *Building an Online Fortress* (Credit Card Management, 2001).
[13] Ibid.

Det finns en mängd tekniska lösningar för bekämpning av kontokortsbedrägerier, som kan integreras i e-handelssystem. Det kan vara svårt för e-handlare att hitta en bra kombination av sådana tekniska lösningar. För att förstå hur bedrägeribekämpning inom Internethandel kan gå till, så kommer ett antal sådana tekniker analyseras och presenteras.

Huvudfrågeställning:
Vilka tekniska lösningar kan e-handlare använda sig av för att bekämpa kontokortsbedrägerier?

Underliggande forskningsfrågor:
- *Vem ligger bakom införandet av den bedrägeribekämpande tekniken?*
- *När en e-handlare använder tekniken, kan han då krävas på kostnaden för en 'chargeback' om ett köp visar sig vara ett bedrägeri?*
- *Lägger tekniken till något extra moment i köpprocessen för kunden?*

Det ligger i kontokortsbolagens intresse att e-handlarna inte drabbas alltför hårt av bedrägerier eftersom e-handlarna är deras kunder. Samtidigt kan kontokortsföretagen tjäna pengar på att ta fram tekniska lösningar för bedrägeribekämpning. Det är därför intressant att veta vem som ligger bakom införandet av en bedrägeribekämpande teknik. Kontokortsföretagen har makt att tvinga e-handlare att använda deras tekniker och dessutom ta betalt av för användningen av dem.[14]

Kostnader för 'chargebacks' kan ge stora ekonomiska konsekvenser, och e-handlare vill givetvis hålla sina kostnader så låga som möjligt. Olika tekniker lägger kostnaden för 'chargeback' på olika aktörer. Till exempel kan användandet av en teknik som ett kontokortsföretag tagit fram flytta över kostnaden från e-handlaren till kortutfärdaren.[15]

Förutom kostnader i samband med användningen av den bedrägeribekämpande tekniken, kan vissa tekniker kräva en extra handling från kundens sida. En teknik som lägger till ett extra moment för kunden, kan leda till att kunder inte slutför sitt tänkta köp. Detta leder i sin tur till minskad försäljning för e-handlaren.[16]

1.3 Avgränsningar

- Vi har inriktat oss på e-handel i form av Internethandel, det vill säga handel mellan företag och privatpersoner. Detta eftersom en privatperson och en e-handlare oftast inte har en inarbetad relation vilket nästan alltid är fallet i handel mellan företag.
- Vi har valt att avgränsa oss till en beskrivning av kontokortsbedrägerier eftersom kontokort är det vanligaste sättet att betala för en vara eller en tjänst över Internet.
- Uppsatsens fokus ligger på global e-handel. Dock har USA en stark position inom e-handeln i världen. Därför kommer mycket av informationen från amerikanska källor. Den baseras även på information om andra länders e-handel, främst från de europeiska.
- I redovisningen av tekniker för bedrägeribekämpning har vi avgränsat oss till de lösningar som tagits fram av kontokortsföretag, systemutvecklingsföretag och e-handlarna själva, detta eftersom det är de här aktörerna samt kortutfärdarna, som uppsatsen fokuserar på.

[14] Paradata Systems Inc: http://www.paradata.com/financial/3ds.htm
[15] http://usa.visa.com/business/merchants/verified_index.html
[16] Efraim Turban, Jae Lee, David King & Michael Chung, *Electronic Commerce, A Managerial Perspective* (2000, Prentice-Hall, Inc, New Jersey).

- Uppsatsen är avgränsad till användningen av kontokort med magnetremsa, och inte kort med chip, så kallade smarta kort. Skälet till avgränsningen är att kort med magnetremsa räknas som standard idag och smarta kort ännu inte slagit igenom inom e-handel. En kortare beskrivning av smarta kort kommer dock ges eftersom smarta kort kan komma att bli en ledande standard i framtiden.
- Secure Electronic Transaction (SET) är en intressant teknik som påminner en del om de tekniska lösningar från kontokortsföretagen som vi presenterat. SET är en teknisk standard för säkra kontokortsbetalningar över Internet. SET kommer inte att behandlas i uppsatsen eftersom SET inte har haft något genomslag bland annat för att tekniken anses som krånglig och framförallt dyr att investera i[17].

1.4 Uppsatsens disposition

I inledningsdelen beskrivs bakgrunden till dess inriktning samt syften och frågeställningar. Här redovisas även de avgränsningar som har gjorts.

Metoddelen inleds med ett avsnitt om kvalitativa metoder och synsätt. I avsnittet finns en illustration av uppsatsarbetets genomförande. Därefter redogörs i ett avsnitt om de insamlingsmetoder som använts för att få tag i information. Metoddelen avslutas därefter med ett avsnitt med metod- och källkritik.

Teoridelen innehåller två avsnitt:

- Den första avsnittet är en översikt över e-handel och Internetbedrägerier. I den här översiktsdelen beskrivs ingående bland annat kontokortsbedrägerier och de olika aktörerna inom e-handel. Beroendeförhållandet mellan aktörerna beskrivs i en modell som vi tagit fram.
- I det andra avsnittet presenteras ytterligare två egenutvecklade modeller. En av modellerna är i punktform och innehåller de aspekter, som vi anser vara viktigast vid e-handlares användning av tekniker för bedrägeribekämpning. Den andra modellen ger en översikt över olika typer av sådana tekniker.

Resultatdelen innehåller följande avsnitt:

- Det första avsnittet analyseras och presenteras tekniker som tagits fram av systemutvecklingsföretag och e-handlare med hjälp av de ovan nämnda modellerna.
- I det andra avsnittet analyseras och presenteras tekniker som tagits fram av kontokortsföretag. Även i den här delen kommer de egenutvecklade modellerna att användas.
- Det tredje avsnittet innehåller presentationer av tre systemutvecklingsföretags e-handelslösningar med bedrägeribekämpande tekniker. Här kommer den egenutvecklade översiktsmodellen att anpassas efter de olika systemlösningarnas innehåll.
- I det fjärde avsnittet redovisas en slutmodell som är sammanslagen av de modeller som använts vid redovisningen av teknikerna. Den visar hur ansvaret för bedrägerier fördelas mellan e-handlare och kortutfärdare.

I diskussionen utvecklas de centrala aspekterna från resultatdelen. Med hjälp av slutmodellen kommer e-handlares situation i dagsläget och i framtiden diskuteras.

[17] Leksell Data: http://www.leksell-data.se/98edis3/set.html

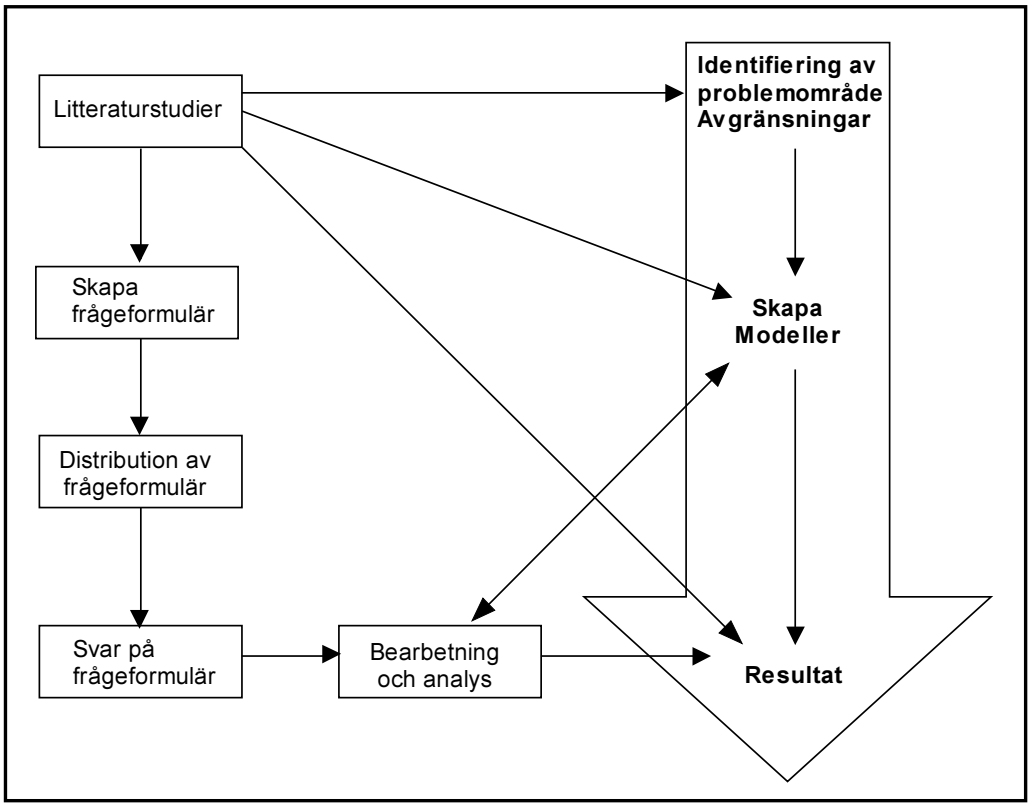
2 Metod

2.1 Vetenskapligt synsätt

Den här uppsatsen och undersökningen baseras på ett kvalitativt synsätt. Detta gäller de metoder som använts för informationsinsamling samt metoderna för bearbetning och analys av informationen. Uppsatsämnet, kontokortsbedrägerier inom e-handel, är ett känsligt område för alla inblandade företag. Vi anser att det krävs mjuka metoder för att skapa förtroende mellan oss som undersökare och företagen som undersökningsobjekt. Kvalitativa metoder kan ge en chans att få djupa och informativa svar om företagens situation vad det gäller bedrägerier och bedrägeribekämpning.

Kvalitativa metoder innebär en låg grad av formalisering. Syftet med sådana metoder är att förstå ett fenomen eller en företeelse. Fokus ligger inte på att pröva om informationen har generell giltighet. Det centrala är att, genom informationsinsamling på olika sätt, få en djupare förståelse av det delområde som studeras. Metoden kännetecknas av närhet till den källa informationen hämtas från.[18]

2.2 Uppsatsarbetets genomförande



Figur 1. Illustration av uppsatsarbetets genomförande

[18] Idar Magne Holme och Bernt Krohn Solvang, *Forskningsmetodik – Om kvalitativa och kvantitativa metoder* (Studentlitteratur, Lund, 1997).

2.2.1 Insamlingsmetoder

- Litteraturstudier
- Sökning efter information på Internet och i databaser
- E-postdistribuerat frågeformulär

Undersökningen inleddes med sökning efter relevant litteratur inom bland annat e-handelsområdet samt bedrägerier och brottslighet på Internet. Detta för att få tag på information om kontokorts-bedrägerier inom e-handel samt bekämpningen av detta problem. I första hand sökte vi efter information i böcker, i andra hand i artiklar och rapporter. Det fanns inga större mängder litteratur att tillgå i biblioteken, varför vi sökte efter information på Internet. Syftet med litteraturstudierna var att ge oss en bred förståelse för hur branschen fungerar, hur utsatt e-handeln är för kortbedrägerier, hur de utförs samt med vilka tekniker de bekämpas. Ur den kunskap som vi införskaffade genom litteraturstudierna och informationen från Internet tog vi fram de tre punkter som blev de fråge-ställningar, som ligger under vår huvudfrågeställning. Punkterna har vi sedan använt för att tydliggöra e-handlarnas beroendeförhållande till kontokortsföretagen och kortutfärdarna i användandet av olika bedrägeribekämpande tekniker.

En annan insamlingsmetod var ett frågeformulär som distribuerades per e-post. Vi ville samla in information från företag som utvecklar lösningar för e-handelssystem. Syftet med den här metoden var att ta reda på hur helhetslösningar för bedrägeribekämpning ser ut. Anledningen till att vi valde den här metoden var att majoriteten av undersökningsföretagen finns i USA eller i Europa, vilket gjorde det omöjligt att genomföra personliga intervjuer på grund av ekonomiska skäl. Planen var att följa upp resultaten från frågeformulären med telefon eller ytterligare e-postintervjuer för att komma närmare våra kontaktpersoner och om möjligt skapa en intressant diskussion. På grund av ekonomiska skäl fick vi begränsa oss till uppföljning enbart per e-post.I informationsinsamlingen genom frågeformulär medverkade sex företag som säljer systemlösningar till e-handlare. En anledning till detta val var antagandet att de testar sina system noggrant, för att kunna ge information till sina kunder. Med andra ord så har de översiktlig information om sina systemlösningar och hur de tacklar bedrägerier.

Några förslag på företag har vi fått från Freddy Tengberg, som fungerat som branschkunnig stödperson för undersökningsdelen av den här uppsatsen. En del av företagen har vi funnit i artiklar från databaser, som till exempel databasen ABI/Inform Global. Valet av undersökningsföretag är baserat på hur lätta företagen har varit att urskilja som stora inom utveckling av e-handelslösningar. Enligt Mehta och Sivadas (1995) så är det att rekommendera att ta kontakt med intressanta respondenter och be om tillstånd innan frågeformuläret skickas ut. Detta ger en högre svars-frekvens.[19] Företagen kontaktades per e-post med en presentation av undersökningsområdet. De företag som var intresserade av att medverka försedde oss med en kontaktperson på företaget. Av nio kontaktade företag tackade sex av dem ja till att medverka i undersökningen. Två av de nio företagen har blivit uppköpta av ett av de medverkande företagen. Ett företag gav ingen respons på frågan om att delta. Kontaktpersonerna hölls informerade om utvecklingen av undersökningsarbetet och frågeformuläret. Därefter distribuerades frågeformuläret per e-post till kontaktpersonerna. Svarstiden var tre veckor, efter två veckor skickades en påminnelse med erbjudande om hjälp vid eventuella oklarheter angående frågorna. Kontaktpersonerna förvarnades om att de kunde komma att kontaktas vid eventuella oklarheter i svaren från frågeformuläret, antingen per e-post eller per telefon. Efter informationsinsamlingen påbörjades bearbetnings- och analysprocessen. Den information som framkom vid litteraturstudierna bearbetades och tolkades iterativt under uppsatsskrivandets gång.

[19] Raj Mehta och Eugene Sivadas, *Comparing Response Rates and Response Content in Mail versus Electronic Mail Surveys* (Journal of the Market Research Society, London, 1995), 37, 4, s. 429-39.

2.3 Metodkritik och källkritik

Validitet och reliabilitet används när teoretiska föreställningar överförs till empiriska observationer. Validitet kan delas in i två olika aspekter: inre och yttre. Att mäta inre validitet är att säkerställa att rätt saker mäts. Den yttre validiteten syftar till att avgöra om det görs på rätt sätt. Förutom validitet finns det andra viktiga krav på ett mätinstrument. Ett sådant är reliabilitet, vilket är ett mått på om ett mätinstrument ger tillförlitliga och stabila utslag. För att uppnå god reliabilitet så skall en undersökning ge samma resultat oavsett vem som utför den.[20]

Under våra litteraturstudier har vi funnit en hel del intressant material. Böcker anses i regel vara tillförlitliga källor. Det visade vara svårt att finna litteratur inom vårt valda område. Därför har vi försökt finna information från andra källor. Vid användningen av material som återfunnits på Internet eller i databaser anslutna till Internet är det av vikt att författarna och framställarna av informationen är tillförlitliga. De artiklar vi använt har vi funnit genom sökningar i GUNDA, Göteborgs universitets biblioteksdatabas. Vid sökningar i den här databasen kan man avgränsa sökningen till att endast omfatta akademiskt granskat material. Den avgränsningen har vi i samband med våra sökningar och därmed anser vi att informationen från de här artiklarna kan betraktas som tillförlitlig. Vi har även använt oss av ett antal rapporter, både av teldokrapporter[21] och rapporter framtagna av marknadsundersöknings- och forskningsföretag vilket är att betrakta som säkra källor. En del information har vi funnit på företags och andra organisationers webbplatser. Vid användning av sådan information har vi försökt vara uppmärksamma samt använda sunt förnuft och försiktighet.

Vi är medvetna om att ett e-postdistribuerat frågeformulär inte är den mest rekommenderade metoden för en kvalitativ undersökning. Eftersom våra undersökningsföretag, geografiskt sett, är lokaliserade långt bort, kan detta ändå ses som ett bra alternativ. När valet står mellan att släppa bra undersökningsobjekt där god kontakt etablerats och påbörja en ny sökning efter intressanta företag, lämpligare placerade geografiskt sett, bör man tänka noga efter. Vi kom fram till att vi ville utnyttja de kontakter som var mest intresserade av att delta i undersökningen oavsett lokalisering, dels på grund av att vi tänkte att deras intresse kunde ge goda resultat, dels för att e-handelsbranschen är att betrakta som internationell.

Respondenterna i undersökningen deltog av olika anledningar. Ett gemensamt skäl till detta var att samtliga respondenter visade stort intresse av ämnet i fråga. Ett annat stort skäl var att få information om hur andra utvecklingsföretag ser på kontokortsbedrägerier inom e-handel. Vi var medvetna om att företagen kunde komma att vara försiktiga när det gällde att lämna ut information om hur bedrägerier hanteras av deras systemlösningar. Det visade sig att de var mer försiktiga än vi hade kunnat förutse. Endast ett företag svarade på samtliga frågor och bara tre företag svarade så pass utförligt att vi kunde redovisa något resultat från dem. Detta trots uppföljningsfrågor och påminnelser per e-post.

I arbetet med vår uppsats har Freddy Tengberg, som vi tidigare varit i kontakt med i form av föreläsare, fungerat som branschkunnig person och bollplank för idéer och funderingar. Vi är medvetna om att hans åsikter kan ha påverkat oss under uppsatsarbetet men anser att vi kontrollerat den information vi inhämtat av honom mot andra källor.

[20] Lars Torsten Eriksson och Finn Wiedersheim-Paul, *Att utreda, forska och rapportera* (Liber Ekonomi, Malmö, 1997).
[21] TELDOK är en oberoende icke-vinstdrivande organisation med syfte att dokumentera praktiska erfarenheter av IT-användning. TELDOK samarbetar med Dataföreningen i Sverige.

2.4 Utvecklingen av egna modeller

Genom litteraturstudier och sökning efter information på Internet har grundläggande kunskap om bedrägeriförebyggande tekniker införskaffats. Kunskapen har använts till att utveckla fyra modeller. De har bland annat använts för att framhäva relevanta aspekter och åskådliggöra resultatet på ett tydligt sätt.

Under litteraturstudierna och bearbetningen av svaren från frågeformulären började vi se ett beroendemönster mellan de olika aktörerna. Vi såg att det förekom en form av hierarki och för att göra detta mer tydligt och överskådligt skapade vi en modell. Den visar hierarkin och beroende-förhållandet mellan huvudaktörerna (e-handlare, kontokortsföretagen, kortutfärdare och system-utvecklingsföretag) och ska öka förståelsen för de inblandades situation. Modellen finns i avsnitt 3.3.1, *Huvudaktörer*, figur 4.

En annan modell består av tre frågor i punktform som tar upp de aspekter som vi funnit mest relevanta ur e-handlares perspektiv angående hur olika bedrägeribekämpande tekniker införs och används. Den finns i avsnitt 4.1, *En modell i punktform*. De frågor som finns i modellen har återkommit regelbundet i den litteratur och annan information vi studerat. Därför valde vi att koncentrera oss på de här frågorna och belysa dem under varje teknik. Det finns naturligtvis en stor mängd relevanta frågor inom området men vi anser att vi valt de som är mest intressanta för uppsatsen. Frågorna fungerar även som underfrågor till huvudfrågeställningen. Vår tanke är att den ska öka förståelsen för e-handlarens situation. I resultatavsnitten 5.1 och 5.2 kommer vi att använda den genom att återge hur varje teknik svarar på frågorna i modellen.

En tredje modell visar en översikt över hur en order behandlas i den del av ett e-handelssystem som innehåller tekniker för bedrägeribekämpning. Den finns i avsnitt 4.2, *En grafisk översiktsmodell*, figur 7. Vi har under litteraturstudien tittat på ett antal systemutvecklingsföretags webbplatser. Flera av dem presenterar sina systemlösningar med hjälp av modeller. Vi insåg att de flesta visade hur en order hanteras genom just deras system.[22] Mönstret i modellen kunde vi även igenkänna när vi studerade svaren från frågeformulären. Baserat på detta byggde vi en mer generell modell över de tekniker vi valt att presentera och diskutera, detta för att läsaren ska kunna få en övergripande förståelse för var i ett bedrägeribekämpande system den redovisade tekniken finns.

Den fjärde modellen är en sammanslagning av översiktsmodellen och modellen i punktform. Den har tagits fram för att samla ihop alla intressanta aspekter från de resultatdelar där de olika teknikerna för bedrägeribekämpning redovisas. Tanken är att den också ska skapa ett intressant underlag för diskussionen. Den finns i avsnitt 5.4, *En sammanslagen slutmodell,* och åskådliggör grafiskt bland annat fördelningen av ansvaret för bedrägerier mellan kontokortsföretag/kortutfärdare och e-handlare vid användning av en viss teknik.

[22] Ett exempel från CyberSource: URL http://www.cybersource.com/resources/seminars/FraudToolsArchive.ppt

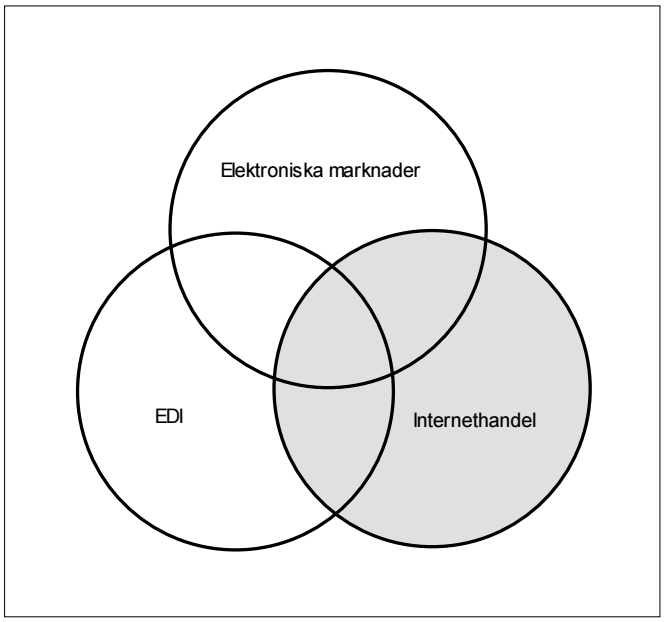
3 Översikt över elektronisk handel och Internetbedrägerier

Det här avsnittet syftar till att ge en beskrivning av elektronisk handel och hur den ser ut idag. I avsnittet beskrivs också de aktörer inom e-handel som uppsatsen omfattar och beroendeförhållandet dem emellan. Dessutom beskrivs två olika typer av kontokort; kort med magnetremsa och så kallade smarta kort. 'Chargeback', återbetalningsprocessen vid felaktiga kontokortsköp redovisas i det här avsnittet i detalj. Avsnittet innehåller även en allmän beskrivning av Internetbedrägerier, med en fördjupning inom området kontokortsbedrägerier. Olika sätt att komma över kontokortsinformation tas upp och av hur stort problemet med kontokortsbedrägerier är.

3.1 Allmänt om elektronisk handel

Elektronisk handel är ett generellt begrepp som innefattar alla former av affärstransaktioner och informationsutbyten som genomförs med hjälp av informations- och kommunikationsteknologi (ICT). E-handel kan ske mellan företag, mellan företag och deras privatpersoner eller mellan företag och offentliga administrationer. Elektronisk handel omfattar handel med varor, tjänster samt elektroniskt material (Esprit, 1997).[23]

Det finns tre olika kategorier av e-handel; EDI, elektroniska marknader och Internethandel (se figur 2).[24]



Figur 2. De tre kategorierna av e-handel. Internethandeln är gråmarkerad eftersom uppsatsen inriktar sig på just den här typen av e-handel
Källa: e-Commerce, Strategy, Technologies and Applications, Whiteley, D., 2000.

[23] David Whiteley, *e-Commerce, Strategy, Technologies and Applications* (The McGraw-Hill Publishing Company, London, 2000).
[24] Ibid.

E-handelssystem omfattar bland annat kommersiella transaktioner på Internet, men deras spännvidd är mycket bredare än så. De kan klassificeras efter vilket användningsområde de tillhör:[25]

- Elektroniska marknader: En elektronisk marknads huvudfunktion är att förenkla sökningar efter varor och tjänster. Det är ett slutet nätverk som endast kan kommas åt av behöriga, det vill säga de som anslutit sig till nätverket genom överenskommelse. Det fungerar som en elektronisk mötesplats där informations- och kommunikationsteknologi används för att visa ett visst utbud inom ett marknadssegment. På en elektronisk marknad kan köpare jämföra exempelvis priser på samt göra inköp av varor och tjänster. Ett exempel på en elektronisk marknad är ett bokningssystem för flygresor där resebyråer, anslutna till just den elektroniska marknaden, bokar resor till sina kunder.

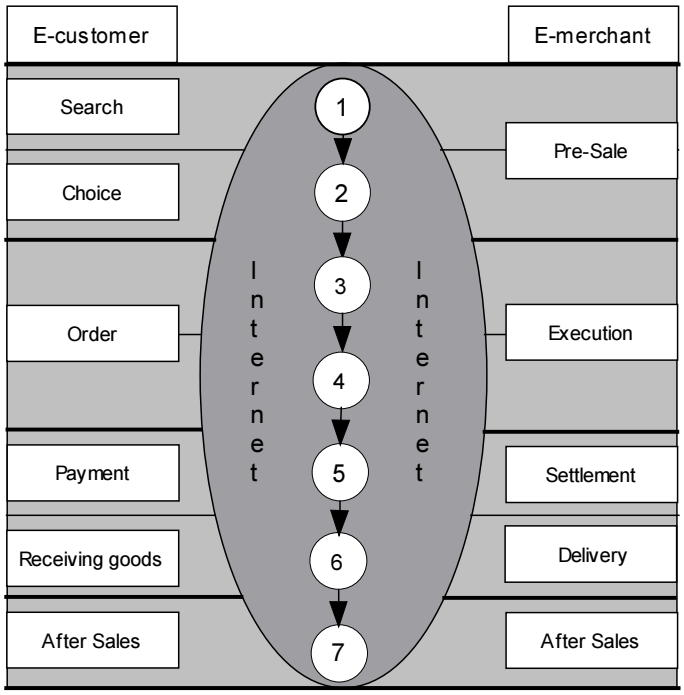
- EDI (Electronic Data Interchange): EDI är ett standardiserat system för att koda affärstransaktioner så att de enkelt kan överföras från ett datorsystem till ett annat utan order och fakturor i pappersformat. Därmed kan de förseningar och fel som ofta följer av manuell pappershantering undvikas. Det handlar om direktöverföring av information mellan två företag.[26] Systemet används av organisationer som har ett stort antal standardtransaktioner och är reglerat genom avtal mellan de inblandade företagen. Det används mycket av större detaljhandlare och fordonstillverkare i kommunikationen med leverantörer.

- Internethandel: Informations- och kommunikationsteknologi kan användas för marknadsföring av och handel med varor och tjänster på Internet. Internet är ett öppet nätverk som vem som helst kan koppla upp sig mot. Den typen av e-handel är ett typexempel på den kommersiella användningen av Internet. Inom Internethandel finns applikationer både för handel mellan företag samt för handel mellan företag och privatpersoner. Exempel på den här typen av e-handel kan vara ett en kund köper en bok på Internet som sedan levereras med post eller bokar biljetter till evenemang som sedan hämtas ut innan evenemanget.

Från och med avsnitt 3.2, Allmänt om Internethandel *kommer vi fortsättningsvis att benämna Internethandel som e-handel.*

[25] David Whiteley, *e-Commerce, Strategy, Technologies and Applications* (The McGraw-Hill Publishing Company, London, 2000).
[26] Efraim Turban, Jae Lee, David King & Michael Chung, *Electronic Commerce, A Managerial Perspective* (2000, Prentice-Hall, Inc, New Jersey).

Händelseförlopp vid e-handel med onlinebetalning (exempelvis med kontokort) :



Figur 3. Händelseförlopp vid e-handel med onlinebetalning
Källa: e-Commerce, Strategy, Technologies and Applications, Whiteley, D., 2000.

Modellen ovan beskriver händelseförloppet vid e-handel över Internet med onlinebetalning i form av exempelvis kontokort. Den tar upp de steg som både e-handlare och e-handelskunder går igenom vid sådan handel. Kunden besöker en e-handelsplats på Internet för att leta efter en viss vara eller tjänst (’search’). E-handlaren lockar till sig kunder genom att en bra och kundvänlig e-handelssida (’pre-sale’). Kunden väljer ut det han vill köpa och fyller i ett orderformulär (’choice’, ’order’). E-handlaren tar emot ordern och kontrollerar att den är korrekt (’execution’). Kunden godkänner att kostnaden för varan eller tjänsten får belastas hans konto (’payment’). När e-handlaren får bekräftelse på att betalningen är godkänd (’settlement’) levererar e-handlaren den beställda varan, antigen elektroniskt eller fysiskt (’delivery’). Därefter levereras varan till kunden, med viss leveranstid (’receiving goods’). Efter det att en försäljning är genomförd kan det fortfarande förekomma kontakt mellan kund och e-handlare (’after sales’). Det kan röra sig om till exempel uppfyllande av garantier, information om varan eller nya produkter från e-handlaren. [27] Vid köpet fyller kunden i ett formulär på e-handlarens webbplats. Den information som kunden ska uppge är som regel namn, adress, telefonnummer, e-postadress, typ av kort, kontokortsnummer och leveransadress.

3.2 Allmänt om Internethandel

Mellan år 2000 och år 2001 ökade antalet e-handelskunder med 50 procent. E-handelskunder som handlade globalt ökade under samma tidsperiod från 10 procent till 15 procent. Internetanvändare som stimulerats till köp i vanliga affärer till följd av besök på e-handelsplatser bidrar också till intäkter för affärsverksamheter. Hela 15 procent av världens Internetanvändare har handlat varor i vanliga butiker på grund av information som de funnit på Internet.[28] Oro över säkerheten på Internet är det största skälet till att inte e-handla för de Internetanvändare som aldrig handlat på Internet. Av

[27] Liu, Jiming & Ye, Yiming, *E-Commerce Agents* (Springer-Verlag, Berlin, 2001).
[28] *Global eCommerce Report 2001* (Taylor Nelson Sofres Interactive, 2001).

de Internetanvändare som aldrig handlat på Internet och som inte har några planer på att göra det är det dels oro för att lämna ut kontokortsuppgifter som hindrar dem, dels oro över generella säkerhetsproblem på Internet.[29]

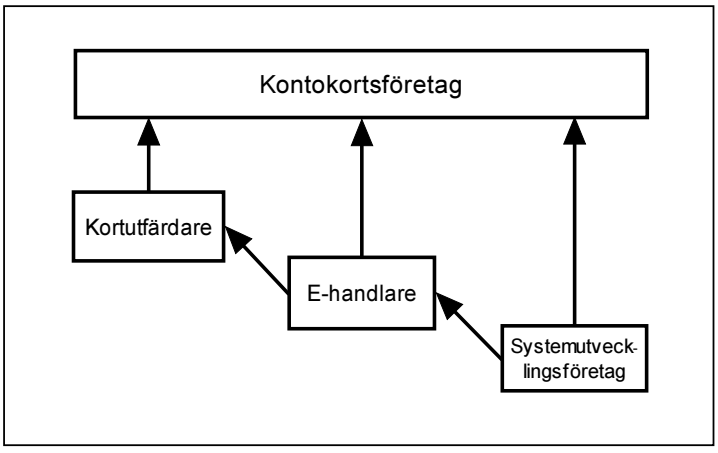
USA är alltjämt världsledande när det gäller procentuell andel av befolkningen som använder Internet för handel och kommunikation. De är även framstående vad det gäller investeringar i den elektroniska infrastrukturen. USAs procentandel av befolkningen som handlar på Internet ligger på 33 procent vilket kan jämföras med det globala medelvärdet på 15 procent. Två länder som sett en stark ökning inom detta område är Tyskland och Storbritannien. Globalt sett så har 55 procent av världens Internetanvändare aldrig handlat på Internet.[30]

3.3 Aktörerna inom e-handel

Följande avsnitt syftar till att ge en översiktlig beskrivning av de aktörer inom e-handel som påverkas av Internetbedrägerier. Aktörerna är de vi har kunnat urskilja under vår undersökning. De aktörer som ingår i en betalning med kontokort är; e-handlare, e-handelskund, kortutfärdare och kontokortsföretag.[31] Systemutvecklingsföretagen besitter stor kunskap när det gäller bedrägerier eftersom de tar fram bedrägeribekämpande tekniker. Branchorganisationerna är sammanslutningar där de flesta av våra aktörer ingår, ofta i samarbete med statliga organ. En ny aktör på marknaden är försäkringsbolagen. Att försäkra sig mot bedrägerier är ett nytt sätt för e-handlaren att skydda sig. Under våra litteraturstudier har vi sett att sambanden mellan vissa aktörer är starkare än mellan andra när det gäller uppsatsen område, bekämpning av kontokortsbedrägerier. På grund av detta har vi valt att dela in de organisationer som vi identifierat som uppsatsens aktörer i två grupper; huvudaktörer och övriga aktörer.

3.3.1 Huvudaktörer

Avsnittet ger en beskrivning av de största kontokortsföretagen, e-handlare, kortutfärdare och systemutvecklingsföretag, samt deras roller inom e-handel och bedrägeribekämpning. Sambandet mellan de har aktörerna är mycket starkt när det gäller framtagandet av tekniker för bekämpning av kontokortsbedrägerier.



Figur 4. Modell över hierarkin och beroendeförhållandet mellan huvudaktörerna

[29] *Global eCommerce Report 2001* (Taylor Nelson Sofres Interactive, 2001).
[30] Ibid.
[31] Efraim Turban, Jae Lee, David King & Michael Chung, *Electronic Commerce, A Managerial Perspective* (2000, Prentice-Hall, Inc, New Jersey).

Vi har tagit fram ovanstående modell för att visa beroendet mellan de olika huvudaktörerna. Kortutfärdarna har slagit sig ihop och skapat kontokortsföretagen. Kontokortsföretagen utvecklar regler, standarder och normer som både kortutfärdare, systemutvecklingsföretag och e-handlare måste anpassa sig till.[32] Därför ligger de i vår modell överst i makthierarkin. En fördel med kontokortsföretagens verksamhet är att e-handelskunder kan handla i hela världen med ett och samma kort. E-handlarna kan ta emot betalningar från hela världen med kort som är anslutna till kontokortsföretagen. Kortutfärdarna sköter kontakten och affärsrelationerna med e-handlarna.[33] Kontokortsföretagen har stor ekonomisk makt över e-handlarna genom att de tar ut avgifter från e-handlarna för användandet av kontokort som betalningsmedel. Kontokortsföretagen kan också tvinga e-handlarna att införa och använda vissa bedrägeribekämpande tekniker.[34] E-handlarnas beroende till kortutfärdarna kommer av att kortutfärdarna, som medlemmar i kontokortsföretagen, har makten att avgöra vilka e-handlare som kan få möjlighet att ta emot kontokortsbetalningar.[35] System-utvecklingsföretagen är i sin tur beroende av e-handlarna eftersom de är potentiella kunder till att köpa deras bedrägeriförebyggande system. De är dessutom i beroendeställning till kontokortsföretagen eftersom systemutvecklingsföretagens tekniska lösningar måste kunna anpassas till kontokortsföretagens tekniker.

Kontokortsföretag

De största kontokortsföretagen är VISA[36], MasterCard[37] och American Express.[38] VISA och MasterCard är sammanslutningar av banker och finansiella institutioner. American Express är ett enskilt börsnoterat företag och utfärdar sina kort själv. Korten fungerar som betalningsmedel hos de handlare som är anslutna till kontokortsföretaget. För debitkort gäller att kortinnehavaren kan handla för det belopp denne har innestående på sitt konto, för kreditkorten gäller att kortinnehavaren får ansöka om en viss kredit hos kontokortsföretaget. När en kund gör ett köp med ett kontokort kontrolleras att kortet är kopplat till ett konto och att kortet är giltigt. Är det inte giltigt blir det en så kallad 'automatic lockout', det vill säga, att kunden nekas till köp.[39] Samtidigt kontrolleras att det finns tillräckligt med medel på kontot för att göra ett köp. Den här kontrollen går genom handlarens kortläsare. Att det är rätt person som handlar med kortet är upp till handlaren att kontrollera.

American Express är ett världsomspännande rese-, finans- och nätverkstjänsteföretag som grundades 1850. Företaget registrerades på New York-börsen 1977 och är idag ett av världens största företag inom kreditkort, resecheckar och resebyråverksamhet.[40] 1999 var American Express, mätt i USD, den största enskilda utfärdaren av kreditkort i USA.[41] American Express har ett så kallat stängt system för betalkort. Detta innebär att American Express äger hela transaktionsprocessen, från det att kortet utfärdas till det att kunden ska faktureras.[42] Vill man som kund ha ett American Express-kort ansöker man om detta direkt hos en av American Express finansiella institutioner. American Express utfärdar inga debitkort utan endast kreditkort.

Visa International Service Association (VISA) är ett privat, vinstdrivande bolag som ägs av omkring 20000 finansiella medlemsinstitutioner från hela världen. VISAs omsättning uppgår till 1445

[32] http://www.MasterCardintl.com/brand/history.html
[33] Kaye Caldwell, *The Public Policy Report* (CommerceNet Newsletter, maj 2001), 3, nr. 5.
[34] Linda Punch, *Building an Online Fortress* (Credit Card Management, 2001).
[35] Matt Mickiewicz & Jim Conley, *Guide to Online Payment Acceptance* (SitePoint.com, 2001).
[36] http://www.visa.com
[37] http://www.MasterCard.com
[38] http://www.americanexpress.com
[39] *Merchant Reports and Tools 3.8* (ClearCommerce, 1999).
[40] http://www24.americanexpress.com/sweden/AboutAmex/about_amex_se_fPress.html
[41] http://www.MasterCardintl.com/about/update/pc_fact.html
[42] Ibid.

miljoner USD globalt (år 1999). VISA, som har sitt huvudsäte i USA, förvaltar VISAs varumärken, fastställer regler för organisationens system och lämnar auktorisations- och clearingtjänster via ett världsomspännande dator- och telekommunikationsnätverk som kallas VISANet. VISA utfärdar inte kort direkt till kunder och ansluter heller inte några köpställen för betalning med VISAkort. Detta sköts av de finansiella medlemsinstitutioner som licensieras för detta av VISA.[43]

MasterCard startade 1966 när en grupp av banker gick ihop och skapade Interbank Card Association. Tanken bakom avtalet var att medlemmarna i organisationen skulle acceptera varandras kontokort. Ur detta utvecklades sedan MasterCard, vars symbol har blivit ett av världens mest igenkända logotyper.[44] Idag är MasterCard en sammanslutning av tusentals finansiella institutioner världen över. MasterCard ger inte ut kort utan det gör medlemmarna, det vill säga kortutfärdarna. Medlemmarna i MasterCard är konkurrenter till varandra och villkoren hos de olika institutionerna varierar.[45]

Både VISA och MasterCard är så kallade öppna system för betalkort. Detta innebär att det kan skilja i faktureringssystem, faktureringssätt och andra faktorer mellan de olika utfärdarna. De olika kortutfärdarna har gått samman och accepterar varandras kort. Konkurrensen mellan kortutfärdarna ökar vilket kan leda till fördelar för kortinnehavarna.[46]

Kortutfärdare

Banker och finansiella institutioner fungerar oftast som utfärdare och distributörer av kontokorten. För att få ett kredit- eller debitkort hos VISA eller MasterCard krävs att man har ett konto på en bank som är ansluten till något av de här kontokortsföretagen. American Express är, som tidigare nämnts, en finansiell institution som utfärdar sina kreditkort själv. Enligt lag i USA[47] är den kortutfärdande banken skyldig att se till att det finns någon sorts mekanism för handlaren att identifiera kortinnehavaren. Det är därför korten har ett utrymme för en signatur på baksidan. Samma lag säger också att kortinnehavaren inte kan hållas ansvarig när kortet inte är närvarande, en så kallad 'card not present'-transaktion. Eftersom utfärdaren inte har gett handlaren något sätt att identifiera en kortinnehavare under en 'card not present'-transaktion, är det egentligen den kortutfärdande banken, som ska stå för kostnaden vid ett bedrägeri. Kortutfärdarna skriver dock över den här kostnaden till e-handlarna genom det avtal e-handlaren måste ingå, för att kunna ta betalt med kontokort.[48] En kund, som hävdar att ett köp som gjorts hos en e-handlare är felaktigt, får pengarna tillbaka. Kortutfärdaren skickar då en 'chargeback' som drabbar e-handlaren. 'Chargeback' är den tekniska termen som används för att beskriva återbetalningsprocessen när ett kortnummer har använts felaktigt. Processen äger rum mellan kortutfärdaren och handlarens bank. Köpbeloppet återförs till kundens konto och e-handlaren debiteras detta belopp samt en administrationsavgift. Den här processen drabbar e-handlarna hårt.[49] 'Chargebacks' presenteras mer utförligt i avsnitt 3.5, *'Chargebacks'*.

E-handelsföretag

Internet är, som bekant, ett globalt nätverk där människor från olika geografiska regioner kan ta del av utbud från en mängd e-handlare, oberoende av var e-handlarna finns lokaliserade. Detta innebär att e-handlarna kan nå och bearbeta även små marknader som tidigare varit olönsamma att etablera

[43] http://europa.eu.int/eur-lex/sv/lif/dat/2001/sv_301D0782.html
[44] http://www.MasterCardintl.com/brand/history.html
[45] http://www.MasterCardintl.com/about/update/pc_fact.html
[46] Ibid.
[47] Regulation Z: URL http://www.federalreserve.gov/boarddocs/press/boardacts/2000/20000928/attachment.pdf
[48] Kaye Caldwell, *The Public Policy Report* (CommerceNet Newsletter, maj 2001), 3, nr. 5.
[49] Jason Klemow, *Credit Card Transactions via the Internet* (TMA Journal, Atlanta, 1999), 19, 1, s. 10–14.

sig i.[50] En självklar fördel vid en global etablering med hjälp av Internet är givetvis den enorma grupp av potentiella kunder, som e-handlare har möjlighet att nå. Detta kan ske till en relativt sett liten investering i tid och pengar jämfört med en fysiskt global etablering.[51] De flesta transaktioner mellan e-handlare och kunder är så kallade 'card not present'-transaktioner. Eftersom det är upp till e-handlaren att bevisa att kunden verkligen har handlat av honom är det e-handlaren som måste ta den största kostnaden för bedrägerier. Dessutom måste e-handlare betala ungefär dubbelt så mycket för varje 'card not present'-transaktion mot vad en vanlig handlare betalar för en 'card-present'-transaktion till kontokortsföretagen.[52]

Systemutvecklingsföretag

Om en e-handlare saknar ett pålitligt system för att upptäcka bedrägerier finns alltid möjligheten att vända sig till ett företag som utvecklar sådana applikationer, vilket dock kan bli mycket kostsamt för e-handlaren. Det kan vara en engångskostnad, en kostnad för varje undersökt transaktion eller både och. De flesta tekniker som systemutvecklingsföretag använder sig av är inriktade på att registrera och utvärdera kundens beteendemönster under den tid som kunden besöker en e-handlares webb-plats. Många systemutvecklingsföretag erbjuder e-handlare helhetslösningar[53] vilket innebär att systemutvecklingsföretagen är tvungna att anpassa sina system, så att även kontokortsföretagens tekniska lösningar kan implementeras. Detta eftersom e-handlarna måste använda vissa tekniker från kontokortsföretagen. Systemutvecklingsföretagen kan alltså inte, som kontokortsföretagen, tvinga sina tekniska lösningar på e-handlarna.

3.3.2 Övriga aktörer

De övriga aktörerna är e-handelskunder, branschorganisationer och försäkringsbolag vilka också berörs också av bedrägerier. De här aktörerna är inte aktiva i framtagandet av bedrägeribekämpande tekniker men är intressanta att beskriva för att få en helhetsbild av problemområdet.

E-handelskunder

Kunder som handlar på Internet gör det av en mängd olika orsaker. Ett skäl är bekvämlighet genom att slippa bege sig till en affär, ett annat skäl kan vara att enkelt kunna göra jämförelser genom att snabbt och lätt kunna granska ett brett utbud. Dessutom finns ofta möjligheten att kunna hitta varor med lägre priser än i vanlig handel.[54] Kunderna är känsliga för komplexitet vid e-handelsköp och kräver att köpet ska kunna genomföras snabbt och enkelt.[55] I en undersökning av Ernst & Young med amerikanska Internetkunder från år 1999 fann man bland annat fyra huvudsakliga drivkrafter som lockade kunder till att handla på Internet:[56]

- Spara pengar genom lägre priser
- Bekvämare, färre resor
- Större urval
- Roligare än att handla traditionellt

[50] Anette Nyström, Maria Kollberg & Johan Eliason, *Internethandel i Europa* (Sveriges Tekniska Attachéer, Stockholm, 1998).
[51] Weje Sandén, *Nätet som marknadsplats: De svenska pionjärerna* (KFB och Teldok: Stockholm, 1998).
[52] Kaye Caldwell, *The Public Policy Report* (CommerceNet Newsletter, maj 2001), 3, nr. 5.
[53] Ett exempel: http://www.buyonet.com
[54] PowerPoint-presentation från Freddy Tengbergs föreläsning på kursen E-handel våren 2001.
[55] Efraim Turban, Jae Lee, David King & Michael Chung, *Electronic Commerce, A Managerial Perspective* (Prentice-Hall, Inc, New Jersey, 2000).
[56] Ernst & Young: http://www.ey.com/global/gcr.nsf/International/International_Home

Fördelar med e-handel för privatpersoner:[57]

- Möjlighet att handla hemifrån – slippa åka, parkera och köa.
- Möjlighet att handla globalt, när som helst på dygnet.
- Utbud av de senaste varorna till låga priser.
- Hemleverans (gäller främst USA).
- Information, service och support lättillgängligt på Internet.

Nackdelar med e-handel för privatpersoner:[58]

- Problem med säkerhetsfrågor gällande skydd av personliga uppgifter och säkra transaktioner.
- Fysiska varor måste levereras vilket kan ge förseningar, besvär och extra kostnader.
- Inga möjligheter att kontrollera varan, till exempel vad det gäller kvalitet.
- Att handla på Internet är ingen social upplevelse.
- Problem vid eventuell retur av varor.

Böcker och CD-skivor är de mest köpta varorna inom e-handeln. Kläder ligger på tredje plats bland vilka typer av varor som säljs över Internet. Utbudet av olika varutyper har breddats, vilket kan bero på att människor känner sig tryggare vad det gäller att handla olika typer av varor över Internet.[59]

I framtidens handel på Internet kommer försäljning av digital information, som kan levereras direkt över nätet, öka kraftigt. Fördelarna med att leverera produkter digitalt över Internet är dels att producenten kan uppnå stora besparingar, och att kunden får sin vara direkt, utan leveranstid.[60] Exempel på digitala produkter kan vara programvaror, musik och filmer. Problemet med detta är att det krävs stor kapacitet vid överföringen, en CD-skiva med musik tar upp cirka 600 megabyte, vilket kräver en nedladdningstid på 40 timmar med ett normalt modem. Det krävs alltså att kunderna har en mycket snabb Internetuppkoppling.[61]

Branschorganisationer

Det finns ett antal olika branschorganisationer som arbetar för att förebygga bedrägerier. I detta avsnitt kommer några av dem att beskrivas, för att visa att det finns en vilja bland aktörerna inom e-handeln att bekämpa bedrägerier.

Merchant Fraud Squad är ett världsomspännande bedrägeriförebyggande nätverk, grundat av bland andra American Express. De försöker reducera e-handlares utsatthet för Internetbedrägerer och stödja tillväxten inom e-handel. Medlemskap är kostnadsfritt. Ett par av medlemmarna är EUROPOL[62], American Express, VISA, Amazon.com, Bank of America, ClearCommerce Corp och CyberSource Corp.[63]

Nätverkets strategier:

- Att tillhandahålla de bästa lösningarna genom att identifiera, utvärdera och rekommendera bedrägeribekämpande lösningar baserat på e-handlarnas behov.

[57] David Whiteley, *e-Commerce, Strategy, Technologies and Applications* (The McGraw-Hill Publishing Company, London, 2000).
[58] Ibid.
[59] *Global eCommerce Report 2001* (Taylor Nelson Sofres Interactive, 2001).
[60] Efraim Turban, Jae Lee, David King &.Michael Chung, *Electronic Commerce, A Managerial Perspective* (Prentice-Hall Inc., New Jersey, 2000).
[61] Johan Gustavsson, *Modeller för betalning på internet* (Högskolan i Örebro, 1996).
[62] Eu-ländernas gemensamma polisbyrå. URL http://justitie.regeringen.se/pressinfo/pdf/FaktaJu_0107.pdf
[63] http://www.merchantfraudsquad.com/pages/members.html

- Att tillhandahålla information för att hjälpa medlemmarna genom att förmedla bedrägeritrender och nyheter inom området.
- Att förbättra säkerheten genom att begränsa e-handlarnas utsatthet för bedrägliga kontokorts-transaktioner.
- Att främja tillväxten inom e-handel genom att öka kunders förtroende för säkerheten med personlig information för att kunna handla säkert över Internet.

APACS (Association for Payment Clearing Services) är en förening vars medlemmar består av, bland andra, bankerna i Storbritannien. Föreningen grundades 1985 och är ett forum för att kunna diskutera icke-konkurrensmässiga frågor för betalningar med bland annat kontokort. En viktig del av APACS arbete med kontokort är bedrägeriförebyggande åtgärder.[64] APACS har en underförening som heter Plastic Fraud Prevention Forum (PFPF) med representanter från de största kortutgivarna i Storbritannien. Även VISA och Europay/MasterCard är medlemmar i föreningen. PFPFs roll är att utveckla och implementera strategier för att förebygga kortbedrägerier. PFPF har regelbundna möten med nyckelpersoner från de stora återförsäljarföreningarna, polisen och ”Home Office”.[65] Home Office är ett statligt verk i Storbritannien som är ansvarigt för inrikesaffärer i England och Wales.[66]

Europeiska Gemenskapernas Kommission har av EUs Parlament blivit uppmanad att föreslå specifika förebyggande åtgärder för att bekämpa bedrägerier och förfalskningar, som rör andra betalningsmedel än kontanter. Detta behövs för att utveckla e-handeln. Ett centralt inslag i handlingsplanen för förebyggande av bedrägeri är ett nära samarbete mellan de berörda myndigheterna och privata parterna, utbyte av erfarenheter och information, utbildning, utveckling och gemensamt undervisningsmaterial.

Kommissionen meddelade den 9 februari år 2001, att den kommer att lansera en ”webbplats för förebyggande av bedrägeri” med information om initiativ som gäller förebyggande av bedrägeri och länkar till andra relevanta organisationer. Man kommer att organisera en konferens för ledande poliser, domare och åklagare för att upplysa om betalningsbedrägerier och deras inverkan på finansiella system.[67]

Försäkringsbolag

Ett relativt nytt fenomen inom e-handelsbranschen är försäkringsbolag som erbjuder e-handlare försäkringar mot Internetbedrägerier. Försäkringsvillkoren är emellertid rigorösa och ställer hårda krav på att e-handlaren har viss hård- och mjukvara för att förhindra bedrägerier.[68] Några försäkringsbolag, till exempel Chubb Group, Lloyds of London, St. Paul Companies och RC Knox & Co, erbjuder försäkringar som inte faller under traditionella databrottsförsäkringar. RC Knox lanserade i juni 2001 en försäkring för e-handlare mot stora kortbedrägerier och ’chargebacks’. För att försäkringen ska gälla måste företagen använda företaget Retail Decisions systemlösning. Försäkringen täcker förluster från stulna kontokort, identitetsbedrägerier och förfalskade kort. Försäkringen går in när förlusterna uppgår till 100 000 USD för en liten e-handlare och 10 miljoner USD för en medelstor e-handlare. För de största e-handlarna går försäkringen in när förlusterna överstiger 250 miljoner USD.[69]

[64] http://www.fraud.org.uk/
[65] http://www.cardwatch.org.uk/
[66] http://www.homeoffice.gov.uk/
[67] http://europa.eu.int/eur-lex/sv/com/cnc/2001/com2001_0011sv01.pdf
[68] RC Knox & Company: http://www.peoples.com/im/cda/rcknox_services/1,,11852,00.html
[69] Linda Punch, *Defending Online Payments* (Credit Card Management, New York, 2001), 14, 7, s. 42-52.

3.4 Kontokort

Idag har de flesta kort en magnetremsa på baksidan av kortet. Så kallade smarta kort håller sakta men säkert på att introduceras över världen. Detta avsnittet innehåller en kort beskrivning av de båda.

3.4.1 Kort med magnetremsa

Den första användningen av magnetremsa på kort var i Londons tunnelbana i början av 1960-talet. På 1970-talet blev magnetremsan standard för kontokort. Idag finns en standard för alla kontokort, för att de ska kunna användas i hela världen.[70] Det traditionella kortet med magnetremsa har blivit en nödvändighet för det vardagliga livet. De används för att ta ut kontanter, handla, tanka med mera.[71] Idag finns en infrastruktur för kort med magnetremsa över hela världen. Kort med magnetremsa är billiga att framställa men har den nackdelen att man inte kan lagra så mycket data på remsan.[72] Lagringskapaciteten för en magnetremsa är cirka 200 bytes. När ett kontokort dras i en kortläsare kan information som namn, kontonummer och giltighetstid avläsas.[73] Kort med magnetremsa kan kopieras mycket lätt (se i avsnitt 3.6.2.1, under rubriken *'Skimming'*).

3.4.2 Smarta kort

Smarta kort är en fransk uppfinning. Roland Moreno, det smarta kortets upphovsman, tänkte sig säkrare bankkort när han tog patent på smarta kort för 23 år sedan. Men den första och största tillämpningen var telefonkorten, som började säljas 1985 i Frankrike. Smarta kort – också kallade aktiva kort – innehåller ”intelligens” i form av ett chip och en mikroprocessor. Mikroprocessorn gör att man kan programmera kortet, processorns minneskapacitet avgör hur många applikationer som får plats. Det smarta kortets minne nås bara av mikroprocessorn och detta ger hög säkerhet. Det smarta kortet går att programmera med ett antal uppgifter så att det kan utföra olika operationer. Det kan till exempel fungera som en elektronisk portmonnä, buss- eller flygbiljett, ett hälsokort med olika medicinska uppgifter, ett elektroniskt ID-kort, ett bankkort, ett telefonkort med mera. Användningsområdena för smarta kort är många. De flesta smarta kort är personliga genom att det krävs en PIN-kod för att kunna användas. Vissa kort är dock opersonliga som till exempel telefonkorten. I slutet av 1992 var alla bankkort smarta i Frankrike, vilket har gjort att bedrägerierna med kort minskat kraftigt.[74] På ett smart kort låses all information om kortinnehavaren med en PIN-kod. Ett smart kort verifierar kortinnehavarens identitet eftersom kopiering av korten idag inte är möjlig.[75]

Kreditkortföretagen Europay, MasterCard och VISA har kommit överens om en internationell standard för smarta bankkort, EMV (en förkortning av Europay, MasterCard och VISA). EMV fastställer normen för kortbetalningar med och automatanvändning av bankernas smarta kort. Införandet av EMV-standard utgör en garanti, för att internationella smarta kort, affärernas betalterminaler samt automaterna fungerar tillsammans på ett säkrare sätt än förut, och att möjligheterna till missbruk minskar drastiskt.[76] American Express har introducerat sitt Blue Card. Ett problem är den nuvarande infrastrukturen av maskiner som är gjorda för att läsa av magnetremsor på korten. Kortläsarna måste bytas ut, och det tar tid och kostar pengar. Ett annat problem är kortläsare för privatpersoner. För att kunna använda säkerheten i smarta kort behöver en kund, som

[70] http://www.aimi.org/technologies/card/magnetic_stripe.htm
[71] http://www.linuxnet.com/info.html
[72] http://www.aimi.org/technologies/card/magnetic_stripe.htm
[73] http://www.aamva.org/Documents/stdBestPracticesMagStripe2dot0.pdf
[74] Ulla-Karin Höynä, *Smarta kort - den smartaste lösningen?* (Teldok Info 17, 1997).
[75] Keycorp Limited:
http://www.keycorp.net/smartcard/What%20will%20drive%20smartcards%20in%20the%20Australian%20marketplace.pdf
[76] http://www.nordea.fi/SWE/info/news/20020215.ASP?navi=yritysinfo&item=yritysinfo

sitter vid sin dator och vill handla på Internet, en kortläsare kopplad till datorn.[77] När en transaktion utförs med smarta kort och en kortläsare behöver handlaren inte stå för kostnaden om transaktionen är ett bedrägeri. Den här kostnaden förflyttas då till kortutfärdaren.[78]

3.5 'Chargebacks'

'Chargeback' är, som tidigare nämnts, den tekniska termen som används för att beskriva återbetalningsprocessen när ett giltigt kortnummer har använts felaktigt. De flesta 'chargebacks' uppkommer genom rena bedrägerier. Det förekommer fall där kunder har beställt varor men sedan nekar till att ha gjort köpet. 80-83 % av 'chargebacks' inom e-handeln kan härledas från transaktioner som inte är gjorda eller är auktoriserade av kortinnehavaren.[79] Vid de flesta 'chargebacks' är dock kortinnehavaren helt oskyldig; det är helt enkelt någon annan som har handlat med dennes kortuppgifter och fått varan skickad till en helt annan adress än kortinnehavarens.[80]

Det är egentligen kortutfärdaren som ska stå för kostnaderna vid 'chargebacks'. När en e-handlare får ett handlarkonto hos en kortutfärdare blir e-handlaren tvungen, genom kontoavtalet, att ta över den juridiska risken för eventuella 'chargebacks'.[81] Bankerna tar ut en påtaglig administrationsavgift för varje 'chargeback' från e-handlarna, vilket kan drabba dem hårt. Meridien Research uppskattade i december 1999 totalsumman för 'chargebacks' i internationell e-handel till 1,5 miljarder USD per år och tillade att problemet kommer öka i takt med e-handelns tillväxt.[82] Avgiften för varje 'chargeback', som e-handlaren måste betala, kan variera mellan 15-50 USD, i USA, beroende på vilket kontokortsföretag det gäller och vad som står i e-handlarens avtal med banken. I Sverige är avgiften för en 'chargeback' från utlandet 800 SEK (MasterCard och VISA) medan avgiften i Storbritannien är 11 GBP (MasterCard och VISA).[83] Vissa e-handlare har till och med gått i konkurs på grund av 'chargebacks' och bankernas avgifter.[84] De e-handlare som är anslutna till VISA får inte ha 'chargebacks' för mer än 2.5 % av omsättningen eller mer än 50 'chargebacks' per månad. Om en e-handlare överstiger gränserna får denne böter på 5000 USD. Om 'chargebacks' fortsätter att ligga över gränsvärdena kan böterna gå upp till 25 000 USD. MasterCard har ett liknande system och deras böter kan uppgå till 100 000 USD.[85]

Enligt Europay International/MasterCard går 'chargeback'-processen till enligt följande: [86]

1. För att få tillbaka pengar för det köp som kortinnehavaren anser felaktigt måste kortinnehavaren skriva till utfärdaren av kortet så fort kortinnehavaren har upptäckt det felaktiga köpet. (Senast inom 180 dagar i Europa, 120 dagar i USA.)

2. Kortutfärdaren analyserar brevet och bestämmer utifrån sina egna regler att antingen:

- Direkt återbetala summan till kortinnehavaren utan att använda 'chargeback'-proceduren. Detta sker oftast om det rör sig om så låga belopp att kortutfärdaren inte anser att det lönar sig att sända en 'chargeback'.
- Sända en 'chargeback' till e-handlarens bank.
- Neka till återbetalning om det bedöms att kortinnehavaren har fel.

[77] Illena Armstrong, *Smartcards: Still a Gamble?* (Scmagazine, oktober 2001).
[78] Adrian Mello, *How Smart Cards Will Revolutionize e-Commerce* (ZDNet News, 14 januari, 2002).
[79] Linda Punch, *Defending Online Payments* (Credit Card Management, New York, 2001), 14, 7, s. 42-52.
[80] Kaye Caldwell, *The Public Policy Report* (CommerceNet Newsletter, maj 2001), 3, nr. 5.
[81] Ibid.
[82] Patricia A. Murphy, *The Murky World of 'Net Chargebacks* (Credit Card Management, New York, 2000), 12, 11, s. 54–60.
[83] Kaye Caldwell, *The Public Policy Report* (CommerceNet Newsletter, maj 2001), 3, nr. 5.
[84] http://europa.eu.int/comm/internal_market/en/ecommerce/chargeback.pdf
[85] Greg Sandoval, *As Net Fraud Grows, So do E-tailers' fears* (CNET News.com, 5 oktober, 2001).
[86] http://europa.eu.int/comm/internal_market/en/ecommerce/chargeback.pdf

3. Om kortutfärdaren väljer att göra en ’chargeback’ sänds den elektroniskt till handlarens bank som kan göra något av följande:
- Debitera e-handlarens konto med köpbelopp samt administrationsavgifter.
- Överklaga med motivering att transaktionen var riktig.

Det vanligaste utfallet från ’chargeback’-processen är en ’chargeback’ till e-handlarens bank och e-handlaren drabbas av kostnaden.[87] Ett problem för e-handlarna är att få den typ av handlarkonto som krävs för e-handel. Som tidigare nämnts, kan en e-handlare som har ’chargebacks’ på över 2,5 % av intäkterna riskera böter och till och med riskera att få sitt handlarkonto avstängt.[88] Detta innebär att man inte kan ta betalt av kunder genom kontokort. Har en handlare väl förlorat sitt handlarkonto hos en kortutfärdare kan detta innebära svårigheter att få ett nytt konto under flera år.[89]

För att sammanfatta kan en e-handlare drabbas av följande under en ’chargeback’-process.
- Förlust av varan som e-handlaren skickat iväg.
- Avgift från kortutfärdaren för ’chargeback’-processen
- Böter från kontokortföretagen

MasterCards ’card not present’-transaktioner är endast 4 procent av alla transaktioner, men de står för 40 % av alla ’chargebacks’.[90]

3.6 Internet- och kontokortsbedrägerier

Generellt sett refererar termen ”Internetbedrägerier” till bedrägerier som använder sig av Internets kommunikationsmedel, som till exempel chattar, e-post och elektroniska anslagstavlor, för att ge bedrägliga förslag till potentiella offer, utföra bedrägliga transaktioner eller för att överföra vinster från bedrägerier till finansiella institutioner eller andra inblandade i bedrägeriet (pengatvätt).[91] Internetbedrägerier är en allvarlig faktor för e-handlare av alla storlekar. E-handlare idag blir mer och mer vaksamma och medvetna om problemet. Det nuvarande ekonomiska klimatet försvårar för e-handlarna att investera i bedrägeriförebyggande tekniker. Enligt en undersökning av företaget Cybersource, som intervjuat 220 e-handlare, anser 57 % av e-handlarna att kontokortsbedrägerier har varit ett allvarligt problem det gångna året. Bedrägerierna tar mycket resurser från personalens övriga arbetsuppgifter. Bedrägliga transaktioner är cirka 3 % i medeltal av försäljningen över Internet år 2001. E-handlarna anser också att de bedrägeriförebyggande systemen ställer till problem för kunderna i form av tidstillägg och extra moment under köpprocessen.[92]

En fördel med kontokort är att kortinnehavaren inte behöver befinna sig på den plats där köpet sker. Det är ett av skälen till att kontokort och framför allt kreditkort är det i särklass vanligaste betalningsmedlet på Internet. En e-handlare som inte tar kontokort har inte troligtvis inte särskilt stora chanser att sälja sina varor utanför landets gränser. Betalning med kontokort är dock inte alltid säkert. En e-handlare som accepterar kontokort utsätter sig själv för en stor risk. Internet är bedragarnas drömvärld eftersom anonymiteten är stor och e-handlarna har svårt att veta om ett kontonummer är stulet eller genererat (se avsnitt 3.6.2, *Olika sätt att komma över kontokortsinformation*). E-handeln håller på att komma ikapp bedragarna med ett antal

[87] Kaye Caldwell, *The Public Policy Report* (CommerceNet Newsletter, maj 2001), 3, nr. 5.
[88] Ellen Messmer, *Credit Crunch for E-comm Wannabes* (Network World, Framingham, 1999), 16, 22, s. 64.
[89] Matt Mickiewicz & Jim Conley, *Guide to Online Payment Acceptance* (SitePoint.com, 2001).
[90] Greg Sandoval, *As Net Fraud Grows, So do E-tailers' fears* (CNET News.com, 5 oktober, 2001).
[91] Bruce D. Mandelblit, *Clicks & Crime: the Inside Story of Internet Fraud* (the Security, Troy, 2001), 38, 9, s. 31–32.
[92] CyberSource: http://www.cybersource.com/fraudreport2001/

bedrägeribekämpande tekniker men på något vis ligger alltid de kriminella ett steg före lagens långa arm.

För e-handlare som säljer digitala produkter uppstår ytterligare ett par problem som inte drabbar de e-handlare som säljer fysiska produkter. Kunden laddar ner produkten direkt och e-handlaren har ingen fysisk adress att kontrollera, endast en IP-adress.[93] Bedragaren kan betala för varan med ett stulet eller ett falskt kontokort och är sedan borta inom ett par sekunder. E-handlaren har väldigt kort tid på sig att godkänna eller stoppa transaktionen. E-handlaren har heller ingen möjlighet att få tillbaka varan. Vissa rapporter tyder på att cirka 20 % av alla transaktioner för digitala produkter är försök till bedrägeri.[94] Andra siffror talar om bedrägeriförsök på upp till 30 %. Siffrorna kan ändras fort; till exempel kan bedrägeriförsöken öka kraftigt när en ny digital produkt lanseras.[95]

3.6.1 Hur stort är problemet?

Kostnaden för kontokortsbedrägerier fortsätter att öka. En marknadsundersökning uppskattade att bedrägerierna kostade e-handlarna mer än 230 miljoner USD under år 1999. Marknadsundersökningsföretaget Meridian Research påstår att kontokortsbedrägerier på Internet uppgick till 9 miljarder USD under år 2001. Under år 2001 uppgick bedrägerier med kontokort i Europeiska Unionen uppskattningsvis till 600 miljoner euro. Det är en ökning med 50 % från år 2000.[96] Enligt APACS ökade bedrägeriförlusterna för 'card not present'-transaktioner i Storbritannien med 94 % mellan år 2000 och år 2001.[97] Meridien Research gav år 1999 ut en rapport som visade att vissa e-handlarkategorier hade bedrägeritransaktioner på upp till 20 % av det totala antalet transaktioner.[98] Det är svårt att få fram tillförlitliga siffror över hur mycket kontokortsbedrägerier kostar företagen. Mörkertalet i statistiken misstänks vara mycket högt. Företagen vill gärna inte gå ut och tala om att de är utsatta för bedrägerier.[99]

3.6.2 Olika sätt att komma över kontokortsinformation

För att kunna handla med ett kontokort krävs inte att kortet är närvarande, vilket innebär att köp med samma kortnummer kan föregå i två världsdelar samtidigt. Själva kontokortet som sådant är inte så viktigt i dagsläget. Det är siffrorna som finns på kortet som är intressanta och de kan bedragare komma över på ett antal olika sätt. I de följande avsnitten kommer några av dem att redovisas.

3.6.2.1 'Skimming'

'Skimming' kallas det när informationen som finns i kortets magnetremsa kopieras och används till att göra falska kontokort eller användas i 'card not present'-transaktioner. Enligt den amerikanska statliga organisationen Commercial Crime Services är detta det snabbaste växande bedrägeriproblemet.[100]

[93] Steve Gillmor, *Business Pay the Price for Online Credit Fraud* (msn.com, 2002).
[94] *To Build Online Business, Build Trust With Online Merchants, Issuers Can Help Merchants Fend Off Devastating Fraud Losses* (Card News, Potomac, 15 december, 1999), 14, 24, s. 1.
[95] Cecile B Corral, *On-line security, payment services aid e-tailers stung by fraud* (Discount Store News, New York, 1999), 38, 8, s. 20-25.
[96] http://europa.eu.int/eur-lex/sv/com/cnc/2001/com2001_0011sv01.pdf
[97] http://www.apacs.org.uk
[98] *To Build Online Business, Build Trust with Online Merchants, Issuers Can Help Merchants Fend Off Devastating Fraud Losses* (Card News, Potomac, 15 december, 1999), 14, 24, s. 1.
[99] Ibid.
[100] http://www.iccwbo.org/ccs/news_archives/2000/skimming.asp

'Skimmers' är elektroniska apparater som används för att kunna läsa data från kortets magnetremsa. Den stulna informationen laddas sedan ner till en dator och överförs sedan till ett tomt kort.[101] 'Skimmern' kan vara lika liten som en personsökare. En 'skimmer' läser all information på magnetremsan, till exempel kortinnehavarens namn, adress, kortnummer och kreditgräns. På Internet kan en 'skimmer' köpas för cirka 400 USD.[102] Att inneha en 'skimmer' är inte olagligt överallt eftersom den bygger på samma teknik som de kortläsare som finns i de flesta affärer.[103]

Figur 5. Exempel på skimmers
Källa: se fotnot [104]

Ett vanligt sätt att komma över kortet för att kunna stjäla kortinformationen är vid restaurangbesök. När kunden lämnar ifrån sig sitt kort för betalning dras kortet en andra gång genom en 'skimmer'.[105] Kortinnehavaren står inte för kostnaden för 'skimming', den kostnaden drabbar kontokortsföretagen. Skimming orsakar dock kortinnehavaren problem och det kan ta tid innan allt ställs till rätta.[106]

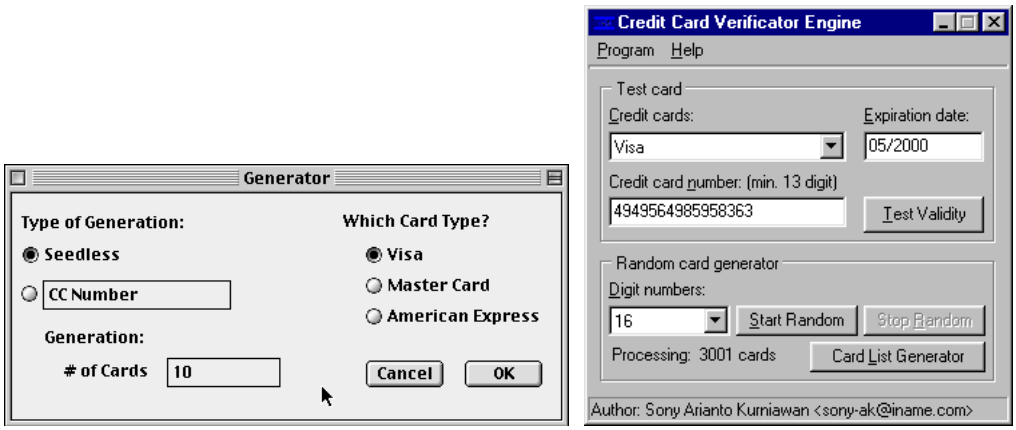
Den totala bedrägeriförlusten för kontokort utfärdade i Storbritannien ökade med 32 % till £373,7 miljoner från årsskiftet 2000/2001 fram till augusti 2001. Av detta stod 'skimming' för 40 % av kostnaden. 'Skimming' är ofta kopplad till organiserad brottslighet.[107] Genom APACSs förening 'Crimestoppers' har man i Storbritannien startat ett projekt som kallas 'Skimming Crackdown'. Detta går ut på att personer som upptäcker 'skimming' kan anmäla detta och få en belöning på £500 om anmälan leder till en fällande dom. Föreningen arbetar också för att få ut smarta kort på marknaden. De smarta korten är i dagsläget så svåra att stjäla information från, så att det inte är ekonomiskt lönsamt att försöka. I slutet av år 2002 räknar APACS med att hälften av alla 108 miljoner kontokort i Storbritannien ska vara smarta kort.[108]

I Kanada uppgick kortförlusterna för banker och återförsäljare till 226 miljoner USD år 2000. Av detta kunde 54 % härröras från 'skimming'.[109]

[101] *Shutting-down Credit Card Fraud* (Pioneer Petroleums News, 14 augusti, 2001).
[102] M Mannix, *High-tech Card Fraud Goes on Right Behind Your Back* (Usnews.com, 2002).
[103] Pennsylvania Maple Syrup: http://www.pennsylvaniamaplesyrup.com/creditcardfraud.htm
[104] *You Can Help Prevent Card Fraud* (E-Advertise, 2000).
[105] http://www.iccwbo.org/ccs/news_archives/2000/skimming.asp
[106] Elaine Shannon, *A New Credit-Card Scam* (Time Europe Magazine Business, 10 juli, 2000).
[107] *Crackdown och credit-card fraud* (BBC NEWS Business, 5 november 2001).
[108] http://www.apacs.org.uk/downloads/skimmingPR.pdf
[109] *Shutting-down Credit Card Fraud* (Pioneer Petroleums News, 14 augusti, 2001).

3.6.2.2 Kontokortsnummergenerering

En mindre sofistikerad metod för att komma över kontokortsnummer är att använda någon av de många program som finns gratis på Internet. Programmen genererar giltiga kortnummer med hjälp av samma algoritmer som används av bankerna. Vem som helst med en vanlig dator och lite grundläggande datorkunskaper kan få fram upp till 999 kortnummer utifrån ett enda kort.[110]



Figur 6. Exempel på ett gränssnitt till en kontokortsnummergenerator
Källa: Se fotnot [111] [112]

Alla kortnummer är baserade på en algoritm. Från början var tanken med algoritmen att man skulle undvika felaktiga inslagningar från affärsbiträden vid manuell inmatning av kontokortsnumret. Generatorn, mjukvaran, skapar kortnummer genom att använda den här algoritmen.[113]
Det är inte svårt att hitta sidor som har kontokortsnummergeneratorer. Här finns två exempel:

- http://www.32bit.com/software/listings/17921/
- http://www.theinformationcenter.com/info1.htm

Det uttrycks klart och tydligt att generatorerna fungerar, men att det är olagligt att använda genererade kontokortsnummer. VISA betalar upp till 1000 USD för information som leder till en fällande dom av någon som är inblandad i tillverkningen eller användningen av genererade kortnummer.[114]

3.6.2.3 Intrång i databaser

Många anser att oron för bristande säkerhet på Internet är överdriven. Men sanningen är att många webbplatser utsätts för intrångsförsök varje dag. För det mesta är ingen skada skedd, men faktum kvarstår; någon har försökt komma åt skyddad data. Ofta vill hackare komma åt information som kontokortsnummer, finansiell information eller orderinformation som kan användas för att skada e-handlaren eller dess kunder. Men ibland vill de bara visa att de kan ta sig in på e-handlarens nätverk.[115] För att kunna ta emot betalning med kontokort över Internet är e-handlarna tvungna att lagra kunders kontokortsdata tillsammans med deras namn och adress. Detta innebär att e-handlare ofta blir utsatta för intrångsförsök från hackare som vill komma åt den här informationen för att

[110] Margaret Mannix, *High-tech Card Fraud Goes on Right Behind Your Back* (Usnews.com, 2002).
[111] http://www.faughnan.com/ccnumgen.html
[112] AriTech Development: http://www.aritechdev.com/ccve/ccve-pic.htm
[113] *Anatomy of an Internet Credit-Card Scam* (BusinessWeek online, 3 april, 2000).
[114] *Restaurateurs BEWARE!* (Food & Service News, 2001).
[115] Informator : http://www.informator.com/Sverige/Allman/Artiklar/Artikel.asp?ArtikelID=9004&ID=245&Aktuellt=45

antingen använda den själv eller för att sälja den vidare till andra.[116] Det finns många exempel på hackare som har åkt fast. Ett sådant exempel är Raphael Gray, en hackare som kallar sig själv Curador. Han ställdes inför rätta för att ha stulit 26 000 kontokortsnummer från flera små e-handlare. FBI uppskattar att förlusterna som kan kopplas till Gray uppgår till 3 000 000 USD.[117]

3.6.2.4 Identitetsstöld

En del Internetbedrägerier innebär ett olagligt anskaffande och användande av någon annans personinformation genom bedrägeri, oftast för att användas vid ekonomiska brott.[118] Identitetsstöld och identitetsbedrägerier är termer som används för att referera till alla sorters bedrägerier som innebär att någon olagligt innehar och använder en annan människas personliga uppgifter för bedrägerier, oftast för ekonomisk vinning.[119] Identitetsstöld var den vanligaste reklamationen som amerikanska konsumenter gjorde år 2001.[120] För de kriminella innebär identitetsstöld en relativt låg risk med möjligheter till stora vinster. Kontokortsutfärdare anmäler oftast inte de kriminella som arresteras eftersom det inte är lönsamt. Företagen har råd att skriva av en del av bedrägerierna. I många stater i USA är identitetsstöld inte ens olagligt.[121] Det främsta skälet till att begå identitetsstöld är för att kunna genomföra kontokortsbedrägerier. Detta leder i sin tur till många 'chargebacks'.[122]

För att få tag på de personliga uppgifterna gör bedragarna allt från att rota i sopor till att hacka hemsidor. Det kan räcka med en kopia av en check eller ett utdrag från ett bankkonto. Internet har blivit ett mycket lönsamt ställe för bedragare att hitta information på. Ett sätt är att skicka e-post där man säger att mottagaren vunnit en resa och det enda mottagaren behöver göra är att svara på mailet med lite uppgifter om sig själv. Ett exempel; en bedragare som stal en identitet, skaffade sig ett kreditkort och spenderade mer än 100 000 USD genom att ta ett lån, köpa ett hus, en motorcykel samt handeldvapen. Han ringde även offret och sa att han kunde fortsätta hur länge han ville eftersom det inte var olagligt. Därefter begärde han offret i personlig konkurs. Det tog offret fyra år och mer än 15 000 USD att få tillbaka sin kredit och sitt rykte. Bedragaren fick ett kortare fängelsestraff för olaga innehav av vapen.[123]

[116] InternetCash: http://www.internetcash.com/fgo/0,1383,white03,00.html
[117] Brian McWilliams, *Welsh Hacker Pleads Guilty to Site Break-ins* (Internetnews.com, 29 mars, 2001).
[118] Bruce D. Mandelblit, *Clicks & Crime: the Inside Story of Internet Fraud* (the Security, Troy, 2001), 38, 9, s. 31–32.
[119] http://www.usdoj.gov/criminal/fraud/idtheft.html#What Are Identity Theft and Identity
[120] *Identity Theft Tops Consumer Fraud Complaints* (Reuters, Tech News, 23 januari, 2002).
[121] http://www.identitytheft.org/
[122] *Online Banking Statistics – Statistics for General and Online Card Fraud* (ePayment Resource Center, 2001).
[123] *What Are Identity Theft and Identity*? (US department of Justice, 2000).

4 Modeller för redovisning av olika tekniker

Syftet med modellerna är att skapa en enkel struktur vid analys och redovisning av de bedrägeribekämpande teknikerna samt vid diskussion av resultatet. Hur modellerna i detta avsnitt har tagits fram och vilken roll de har beskrivs närmare i avsnitt 2.4, *Utvecklingen av egna modeller*.

4.1 En modell i punktform

Modellen i punktform belyser på ett enkelt sätt tre aspekter på hur bedrägeribekämpande tekniker kan användas som e-handlaren måste ta hänsyn till. De tre frågor som ska besvaras i redovisningen av de olika teknikerna är följande:

- Vem ligger bakom införandet av den bedrägeribekämpande tekniken?
  - E-handlaren och/eller systemutvecklingsföretaget
  - Kontokortsföretagen

- När en e-handlare använder tekniken, kan han då krävas på kostnaden för en 'chargeback' om ett köp visar sig vara ett bedrägeri?
  - Ja
  - Nej

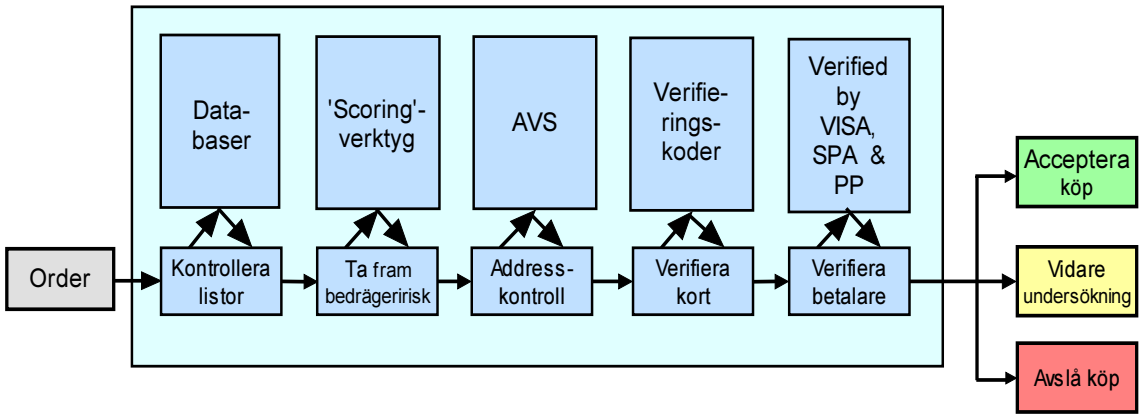
- Lägger tekniken till något extra moment i köpprocessen för kunden?
  - Ja
  - Nej

Vem som ligger bakom införandet av tekniken kan vara en viktig faktor. Vissa bedrägeribekämpande tekniker blir e-handlare mer eller mindre tvingade att använda av kontokortsföretagen. Använder e-handlaren inte tekniken kan denne få högre avgifter, böter eller till och med bli avstängd.[124] En annan fråga som vi anser är viktig är om e-handlare, som använder tekniken, får stå för kostnaden för 'chargeback' om ett köp visar sig vara bedrägeri.

Vissa tekniker som kontokortsföretagen tvingar på e-handlarna kan visserligen begränsa bedrägerierna, men om ett bedrägeri slinker igenom kontrollen står e-handlaren fortfarande där med kostnaden för bedrägeriet och kostnaden för 'chargeback'.[125] De flesta tekniker som kontokortsföretagen har initierat är mest inriktade på att kontrollera att kundens identitet är den rätta. De tekniker som systemutvecklingsföretagen erbjuder e-handlare är mer inriktade på att registrera kundens beteende under själva köpprocessen. Vissa av teknikerna märker inte kunderna av alls. Andra tekniker kräver att kunden lämnar extra information under köpprocessen eller registrerar sig på en speciell webbsida innan denne handlar. Extra steg för kunden under köpprocessen kan påverka om denne slutför sitt köp eller inte. Detta är, av ekonomiska skäl, en viktig faktor att ta hänsyn till för e-handlaren.[126]

[124] Linda Punch, *Building an Online Fortress* (Credit Card Management, 2001).
[125] Paradata Systems Inc: http://www.paradata.com/financial/3ds.htm
[126] Efraim Turban, Jae Lee, David King & Michael Chung, *Electronic Commerce, A Managerial Perspective* (Prentice-Hall, Inc, New Jersey, 2000).

4.2 En grafisk översiktsmodell



Figur 7. Översiktsmodell över olika tekniker för bedrägeribekämpning.

Den grafiska översiktsmodellen ovan visar hur en order kan hanteras i ett system för att begränsa bedrägerier. Ordern behandlas i olika steg efter en viss förutbestämd ordning. När ordern har gått igenom systemet avgörs om ordern ska accepteras, avslås eller undersökas vidare. De olika rutorna innehåller de fem grupper av tekniker som presenteras samt deras grundfunktioner, till exempel ’scoring’-verktyg, en teknik vars huvudfunktion är att ta fram hur stor risken för bedrägeri är. Samtliga delar i modellen behöver inte finnas med i alla system och det finns även funktioner i verkliga system som inte finns med i modellen. Detta är en generell modell som ska ge en uppfattning om hur bedrägerikontroll kan gå till och i vilken ordning en order kan behandlas om flera tekniker finns i ett system. Bedrägeribekämpande tekniker används sällan enskilt utan ofta i kombination med andra tekniker. Därför är det intressant att visa en tekniks placering och uppgift i en helhetslösning.

Det finns ytterligare en modell men eftersom den är en vidareutveckling utav de ovanstående modellerna har vi valt att presentera den först då den ska användas i avsnitt 5.4, *En sammanslagen slutmodell*.

5 Resultat

I resultatet analyseras och presenteras två grupper av tekniska lösningar för bedrägeri-bekämpning. Den ena gruppen av tekniker är framtagen av e-handlare och system-utvecklingsföretag, den andra gruppen är framtagen av kontokortsföretag. Dessutom innehåller resultatavsnittet presentationer av tre systemutvecklingsföretags e-handels-lösningar med bedrägeribekämpande tekniker och en slutmodell som är sammanslagen av de modeller som använts vid redovisningen av teknikerna.

5.1 Tekniker för bedrägeribekämpning från e-handlare och systemutvecklingsföretag

I avsnittet analyseras och presenteras ett antal olika tekniker i e-handelslösningar som används för att förhindra bedrägerier. De tekniska lösningarna kan erbjudas till e-handlare av olika systemutveck-lingsföretag, men e-handlaren kan även utveckla dem själv, om kunskap finnes. Presentationen av de olika lösningarna är endast allmän och grundläggande. Det finns fler lösningar, och många kombineras med varandra för att få ett bättre skydd. Anledningen till att vi valt att presentera de här teknikerna är att de ofta förekommit under vår informationsinsamling. Teknikerna bygger på kunders historiska data eller hur kunder beter sig inne på e-handlarens webbsida.

5.1.1 Databaser

De flesta e-handlare har någon form av databaser. De kan vara egenutvecklade eller framtagna med hjälp av ett systemutvecklingsföretag. Databaserna kan användas till att kontrollera relevant information mot listor som lagras i databaser och, i vissa fall, hjälpa till att bekräfta kunders identitet. Databaser kan också användas som en källa för att kontrollera kundens tidigare transaktioner, till exempel om kunden orsakat många 'chargebacks' eller utfört bedrägerier. En fördel med kontroll av kunders uppgifter mot databaser är att kunderna inte märker att de blir granskade. Det krävs heller ingen handling från kundernas sida vid användningen av den här tekniken.

Det används i allmänhet två sorters databaser:[127]

- Negativa databaser
- Positiva databaser

I båda typerna av databaser kan en e-handlare samla kundinformation som till exempel namn, fakturerings- och mottagaradress, telefonnummer med mera. Dessutom kan information om kunders tidigare köp sparas. I den negativa databasen lagras alla "problemkunder" och deras köp. I den positiva databasen lagras alla kunder som har genomfört köp utan problem.[128] Varje transaktion som tas emot kontrolleras sedan mot den negativa databasen. Har kunden en historia i databasen kan e-handlaren stoppa transaktionen. Fler och fler e-handlare går nu ihop och skapar gemensamma negativa databaser.[129] Det svåra med delade databaser kan vara att alla e-handlare inte har samma kriterier för vad det är som är negativt. Dessutom är delade databaser inte tillåtet enligt lag överallt.[130] Om kontokortsnumret är stulet från en kund som finns i den positiva databasen, kan detta göra att ett bedrägeri lättare släpps igenom. Databaserna måste underhållas hela tiden, annars kan de bli inaktuella och förlora sin effektivitet.[131] Om det är en förstagångskund som handlar har databaser

[127] *Online Card Payments: Fraud Solutions Bid to Win* (Meridien Research, e-Payments, 18 januari, 2001).
[128] Ibid.
[129] Paradata Systems Inc: http://www.paygateway.com/tech/references/fraud.html
[130] E-postintervju med Alan Scutt, VD för ClearCommerce i Europa.
[131] Accept Credit Cards Real Time.Com: http://www.acceptcreditcardsrealtime.com/fraud.htm

liten effekt. E-handlaren får själv stå för de kostnader som uppkommer vid bedrägerier och 'chargebacks' vid användningen av databaser.

- Vem ligger bakom införandet av den bedrägeribekämpande tekniken?
  - E-handlaren och/eller systemutvecklingsföretaget

- När en e-handlare använder tekniken, kan han då krävas på kostnaden för en 'chargeback' om ett köp visar sig vara ett bedrägeri?
  - Ja

- Lägger tekniken till något extra moment i köpprocessen för kunden?
  - Nej

5.1.2 'Scoring'-verktyg

Det finns tre vanliga metoder, så kallade 'scoring'-verktyg, som används för att bygga bedrägeribekämpande system:

- Regelbaserade system
- Logistikregression
- Artificiella neurala nätverk

E-handlare kan äga och använda de här systemen själva och ligger därmed bakom införandet av 'scoring'-verktyg. E-handlare kan också betala ett systemutvecklingsföretag för att utveckla och/eller hantera hela deras e-handelsprocess inklusive bedrägerikontrollen. Vid användningen av 'scoring'-verktyg kommer företagets samtliga transaktioner att kontrolleras. Om kontrollen inte tar för lång tid märker kunden inget. Varje kontrollerad transaktion får en resultatsiffra som är ett mått på hur hög risken för bedrägeri är. Ju högre resultat, desto högre är sannolikheten att transaktionen är ett bedrägeriförsök. E-handlaren kan själv välja på vilken nivå denne vill ha sin acceptansgräns. En transaktion vars resultatsiffra är högre än e-handlarens valda acceptansgräns bör tas om hand för att man inte ska förlora hederliga kunder. Detta kan ske genom mail eller att man helt enkelt ringer upp kunden. E-handlaren vill naturligtvis ha så lite undantagsbehandling som möjligt eftersom detta kostar pengar i form av tid och personalresurser.[132] Detta innebär en svår balansgång för e-handlaren eftersom han vid ett eventuellt bedrägeri får stå för kostnaden och 'chargebacks'. Det krävs en hel del arbete innan en e-handlare hittar en bra acceptansgräns där han stoppar tillräckligt många bedrägerier men antalet undantagsbehandligar är så få som möjligt. Historiska data från de negativa och positiva databaserna kan användas när man bygger 'scoring'-verktyg.

- Vem ligger bakom införandet av den bedrägeribekämpande tekniken?
  - E-handlaren och/eller systemutvecklingsföretaget

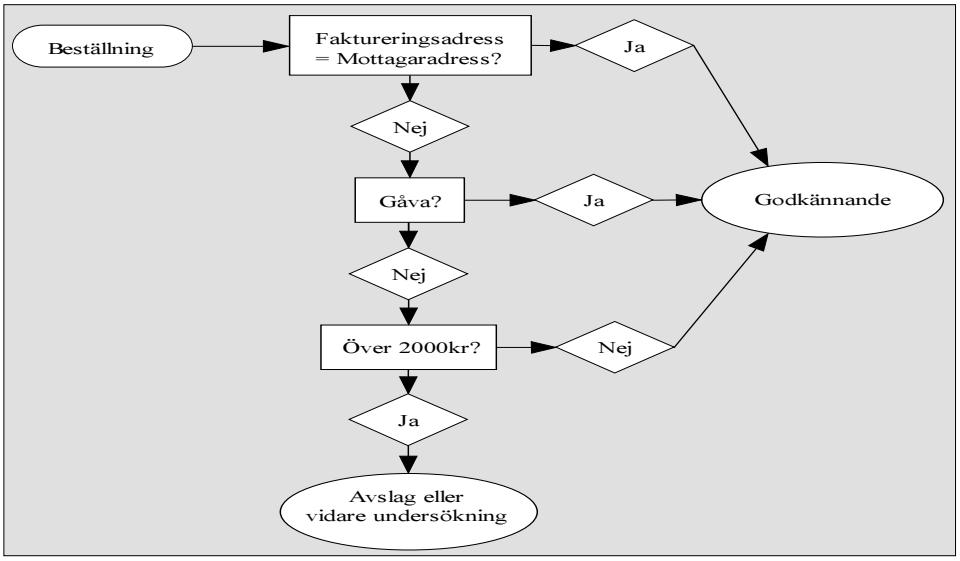
- När en e-handlare använder tekniken, kan han då krävas på kostnaden för en 'chargeback' om ett köp visar sig vara ett bedrägeri?
  - Ja

- Lägger tekniken till något extra moment i köpprocessen för kunden?
  - Nej

[132] Westland, J.C, & Clark, T. H. K. *Global Electronic Commerce*. (Massachusetts Institute of Technology, 2000).

5.1.2.1 Regelbaserade system

Den andra vanliga teknologin är regelbaserade system som använder logik för att komma fram till slutsatser, baserade på ingångsdata. Regelbaserade system bör byggas av experter med kunskap om kännetecken för både bedrägliga och riktiga transaktioner. Det kan vara kunskaper som, till exempel, att en förstagångskund som handlar är en större risk för e-handlaren än en kund som är känd. Det är viktigt att löpande utvärdera de regler som finns i systemet. Reglerna bygger på bedrägeritrender, och när de trenderna förändras måste också reglerna i systemet förändras.[133]



Figur 8. Exempel på ett mycket enkelt regelbaserat system.
Källa: Meridien Research, *Online Card Payments: Fraud Solutions Bid to Win.*

5.1.2.2 Logistikregression

Logistikregression är ett statistiskt synsätt, som används för att förutsäga sannolikheten av ett eller flera utfall med hjälp av matematiska ekvationer, som utvärderar riskvariabler. Logistikregression är väl anpassat för att ta fram ett matematiskt värde, en bedrägeripoäng, som anger risken för att en transaktion är bedräglig. Alla oberoende uppgifter som kommer in i systemet utvärderas. Uppgifterna slås sedan ihop för att få en relativ sannolikhet för att transaktionen är ett bedrägeri.[134]

Ett exempel:
Om mottagaradressen och faktureringsadressen inte stämmer överens, hur stor är då sannolikheten att det rör sig om ett bedrägeriförsök?

- Det är en gåva och priset är under 2000 kr. Sannolikhet = 30 %
- Det är inte en gåva och priset är under 2000 kr. Sannolikhet = 40 %
- Det är en gåva och priset är över 2000 kr. Sannolikhet = 50 %
- Det är inte en gåva och priset är över 2000 kr. Sannolikhet = 80 %

En av fördelarna med logistikregression är möjligheten att följa resultatet av informationen tillbaka igenom systemet och därmed kunna se vilka variabler som var mest relevanta för resultatet.[135]

[133] *Online Card Payments: Fraud Solutions Bid to Win* (Meridien Research, e-Payments, 18 januari, 2001).
[134] Edward C. Malthouse, *ScoringModels* (Medill School of Journalism, Northwestern University, USA, 2002).
[135] *Online Card Payments: Fraud Solutions Bid to Win* (Meridien Research, e-Payments, 18 januari, 2001).

5.1.2.3 Artificiella neurala nätverk

Artificiella neurala nätverk försöker efterlikna den mänskliga hjärnans fysiska uppbyggnad. Man försöker skapa mönster som kan kännas igen som objekt. Precis som den mänskliga hjärnan lär från erfarenhet, kan ett nätverk av den här typen tränas till att känna igen mönster. Neurala nätverk ligger bakom lösningar som till exempel teknologi för att identifiera fingeravtryck, fatta kreditbeslut och system för röstigenkänning. Ett neuralt nätverk måste tränas med kända data. För att upptäcka kontokortsbedrägerier behöver nätverket tränas med både bedrägliga och tillförlitliga transaktioner. Under träningen lär det neurala nätverket sig att känna igen mönster, som indikerar potentiella bedrägeriförsök.[136] Dessa mönster formar grunden av objekt, som kommer att användas för att testa framtida transaktioner. Det är mycket viktigt att nätverket tränas med tillräckliga och relevanta data. När nätverket är klart för att tas i bruk, jämförs alla nya data med existerande mönster. Vissa neurala nätverk kan göra förändringar i mönstret utan tillsyn och blir bättre med tiden. Andra behåller sina mönster och måste uppdateras, för att inte tappa i effektivitet. En nackdel med neurala nätverk kan vara att det är svårt att veta vilken information som leder till ett visst resultat.[137]

[136] *Neural Networks Applied to Direkt Marketing* (Sentient Machine Resarch B.V: Amsterdam, King's College London, 2000).
[137] Kishan Mehrotra, Chilukuri K. Mohan & Sanjay Ranka, *Elements Of Artificial Neural Networks* (Massachusetts Institute of Technology, 1997).

5.2 Tekniker för bedrägeribekämpning från kontokortsföretag

I detta avsnitt analyseras och presenteras tre av de största kontokortsföretagens (VISA, MasterCard och American Express) tekniska lösningar för bedrägeribekämpning. Kontokortsföretagen arbetar också med att stoppa bedrägerierna. Ibland förekommer det samarbete mellan de olika kontokortsföretagen. Vissa av teknikerna fungerar bara i USA, men flera har introducerats eller är på väg att introduceras i Europa. De tekniker som vi tar upp är de tekniker som företagen själva marknadsför på sina hemsidor. Teknikerna har även varit starkt representerade under vår informationsinsamling.

5.2.1 AVS – 'Address Verification System'

AVS är en teknik som kontrollerar att den adress kunden har angivit som faktureringsadress stämmer överens med kontokortsinformationen.[138] År 1996 introducerade VISA och MasterCard en föreskrift för alla amerikanska handlare som handhar 'card not present'-transaktioner. Föreskriften kräver att e-handlarna ska använda AVS vid sådana transaktioner. Om e-handlarna inte accepterar villkoren belastas de med en extra avgift på 1,65 % per transaktion.[139] VISA tar ut en avgift på 0,02 USD för varje transaktion där AVS används.[140] Trots att e-handlarna måste använda AVS får de fortfarande stå för bedrägerikostnader och 'chargebacks'. AVS fungerar bara i USA, så om mottagaradressen ligger utanför USA är det svårt att kontrollera om den angivna adressen är en verklig adress. Detta har att göra med vilka uppgifter som finns lagrade i bankens databas tillsammans med kontokorts-informationen. I USA finns all kundinformation lagrad tillsammans med kontokortsinformationen. I exempelvis Sverige är detta inte möjligt på grund av att bankernas system från början inte var uppbyggt på detta sätt.[141] Förändringar är dock på gång, till exempel kommer AVS att introduceras i Storbritannien inom en snar framtid.[142] Detta är möjligt genom en ny lag, som behandlar hur och vilken personinformation får lagras. Lagen trädde i kraft den 1 mars år 2000.[143]

Förutom att kontrollera kortinnehavarens adress, kan även kortinnehavarens namn och telefon-nummer kontrolleras.[144] AVS kontrollerar dock inte hela adressen. Om kortinnehavarens adress är Kungsgatan 23 och den inmatade adressen är Vasagatan 23 kommer AVS att släppa igenom detta. AVS jämför även kortinnehavarens adress med den angivna leveransadressen. Kunden märker aldrig att denne kontrolleras genom AVS. Eftersom AVS jämför transaktionsdatan med en databas stoppar AVS genererade kontokortsnummer.[145]

Enligt företaget CyberSource blir över 10 % av kunderna stoppade av AVS. Många av de här kunderna är inte bedragare men deras uppgifter stämmer inte överens med kontokortföretagets databas.[146] Ett annat företag, ClearCommerce, har gjort en analys som visar att AVS endast godkänner cirka 40 % av alla transaktioner. Detta innebär att många av transaktionerna som stoppas är inte bedrägerier. En annan viktig faktor är att 35 % av de bedrägerifall som ClearCommerce undersökt har godkänts av AVS.[147]

[138] MerchantSeek: http://www.merchantseek.com/glossary.htm
[139] http://www.dmsontheweb.com/faqs.php
[140] http://www.people.virginia.edu/~slb/avs.html
[141] E-postintervju med Freddy Tengberg, VD för Buyonet
[142] WorldPay Plc: http://www.worldpay.com/uk/news/2001/news_fraudadvice.shtml
[143] http://www.dwp.gov.uk/publications/dwp/2001/gl33.pdf
[144] http://www.clearcard.com/support/avs.html
[145] http://www.clearcard.com/support/avs.html
[146] CyberSource:
http://apps.cybersource.com/library/documentation/product_information_guides/Smart_Authorization_Planning_Guide/html/appA.html
[147] http://www.merchantfraudsquad.com/Members/membpages/fergerson0101.asp#anchor2

Ett exempel på hur man kan ta sig runt AVS:
En bedragare med ett stulet kontokort kan ange kontokortsinnehavarens mottagaradress när han handlar. Sedan kontaktar man e-handlaren och ber om numret på försändelsen, ett så kallat 'tracking number'. Bedragaren kan sedan kontakta fraktföretaget och ändra leveransadressen.[148]

- Vem ligger bakom införandet av den bedrägeribekämpande tekniken?
  - Kontokortsföretagen

- När en e-handlare använder tekniken, kan han då krävas på kostnaden för en 'chargeback' om ett köp visar sig vara ett bedrägeri?
  - Ja

- Lägger tekniken till något extra moment i köpprocessen för kunden?
  - Nej

5.2.2 Verifieringskoder

När en 'card present'-transaktion görs hos en traditionell handlare, avläses magnetremsan på baksidan av kortet med en kortläsare. VISA, MasterCard och American Express har en kod inbäddad i informationen på sina korts magnetremsa. Koden kan användas för att verifiera att det är ett riktigt kort. Kortutfärdarna använder VISAs Card Verification Value (CVV), MasterCards Card Validation Code (CVC) eller American Express Card Identification Number (CID) för verifiering av konto-kortet under auktoriseringskontrollen under en 'card present'-transaktion.[149]

CVV2, CVC2 och CID är en kod som är tryckt på antingen baksidan eller framsidan av kontokortet. Vid en 'card not present'-transaktion ber handlaren kunden ange den här koden. Fortsättningsvis kommer de här koderna att hänvisas till som verifieringskoder.

Figur 9. Placeringen av verifieringskoderna på VISA- och MasterCard-kort
Källa: Se fotnot [150]

Alla MasterCards kort från och med 1 januari år 1997 har en CVC2-kod och alla VISA-kort från och med 1 januari år 2001 har en CVV2-kod. De båda koderna är tresiffriga, tryckta på baksidan av kortet och fungerar på samma sätt trots att de har olika namn. CVV2- och CVC2-koderna bygger på en matematisk algoritm som bygger på kortnumret och kortets giltighetstid.[151] Så länge algoritmen inte är känd kan verifieringskoderna inte fabriceras.[152]

[148] ClearCommerce: http://www.clearcommerce.com/press/articles/wrong_number.html
[149] http://atlanticpayment.com/CVV.htm
[150] *What is CVV2/CVC2 Code?* (FONBET Corp, 2001).
[151] Payment Technologies: http://www.paytech.ru/eng/cvc2.asp
[152] http://swiss-bank-accounts.com/e/faq/CVV2.html

Figur 10. Placeringen av verifieringskoderna på American Express-kort
Källa: Se fotnot [153]

American Express verifieringskod är fyrsiffrig och heter CID. Verifieringskoden finns tryckt på framsidan av korten.[154]

Verifieringskoderna har införts av kontokortsföretagen och är till för att e-handlarna ska kunna säkerställa att det är ett riktigt kort som används i en transaktion. Om någon kommer över ett giltigt kontokortsnummer så kan denne ändå inte använda det för att handla med. Har man inte kortet i sin hand kan man inte ange verifieringskoden som finns på kortet.[155] Om det är så att kontokortsnumret inte stämmer överens med verifieringskoden som kunden angett så har e-handlaren möjlighet att stoppa transaktionen och leveransen av varan.[156] Men e-handlaren måste fortfarande ta kostnaden för 'chargebacks' om det visar sig att en transaktion är ett bedrägeri. Cathy Black, ansvarig för förebyggandet av bedrägerier på American Express, hävdar att metoden är en succé. Med den rätta koden kan handlarna vara tämligen säkra på att kunden inte fått kortnumret och kortets giltighets-datum från ett kvitto, från en kortnummergenerator eller genom 'skimming'.[157] Verifieringskoder anses kunna minska antalet 'chargebacks' med upp till 26 % för e-handlare.[158]

- Vem ligger bakom införandet av den bedrägeribekämpande tekniken?
  - Kontokortsföretagen

- När en e-handlare använder tekniken, kan han då krävas på kostnaden för en 'chargeback' om ett köp visar sig vara ett bedrägeri?
  - Ja

- Lägger tekniken till något extra moment i köpprocessen för kunden?
  - Ja

[153] Wild West Electronics.com: http://www.wildwestelectronics.net/ccv2cidin.html
[154] http://home5.americanexpress.com/merchant/resources/articles/retail5.asp
[155] http://swiss-bank-accounts.com/e/faq/CVV2.html
[156] Payment Technologies: http://www.paytech.ru/eng/cvc2.asp
[157] Ken Clark, *In the War on Fraud, a Call for Teamwork* (Chain Store Age, 2000), 76, 11, s. 116–117.
[158] http://atlanticpayment.com/CVV.htm

5.2.3 'Payer Authentication'-tekniker

'Payer Authentication'- tekniker används för att kortutfärdarna ska kunna verifiera en kortinnehavares identitet för en e-handlare under köpprocessen.[159] E-handlare kan få en bekräftelse på att det är den verkliga kortinnehavaren som vill handla.[160]

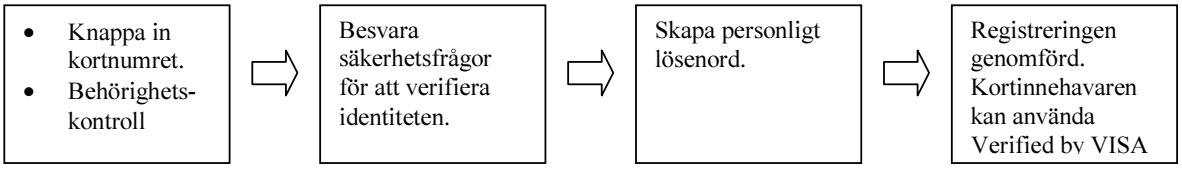
- Vem ligger bakom införandet av den bedrägeribekämpande tekniken?
  - Kontokortsföretagen

- När en e-handlare använder tekniken, kan han då krävas på kostnaden för en 'chargeback' om ett köp visar sig vara ett bedrägeri?
  - Nej

- Lägger tekniken till något extra moment i köpprocessen för kunden?
  - Ja

5.2.3.1 Verified by VISA

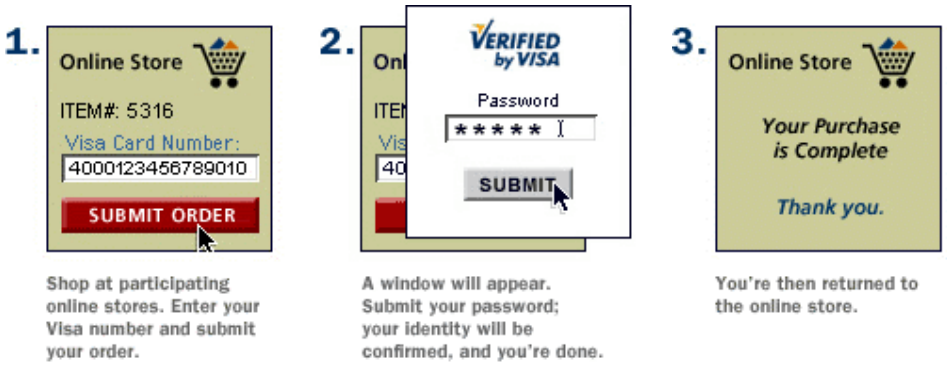
Detta är en gratistjänst för kortinnehavare. Kortinnehavarna behöver inte skaffa sig ett nytt kort utan kan använda det gamla kortet. Dock krävs det att man registrerar sig, för att få tillgång till tjänsten. För att göra detta går man in på Verified by VISAs hemsida.[161] Där går man igenom följande steg:



Figur 11. Registreringsprocedur för Verified by VISA
Källa: Se fotnot [162]

Om kortinnehavaren glömmer bort sitt lösenord måste han ta kontakt med kortutfärdaren.[163] När en kortinnehavare är medlem i Verified by VISA och handlar hos e-handlaren som är ansluten till Verified by VISA kommer kortinnehavaren, när han klickar på "köp", att få upp ett fönster där han ombedes att ange sitt lösenord. Kontrollen tar cirka 10–15 sekunder.[164] Kortinnehavaren behöver inte ladda ner någon mjukvara. Mjukvaran ligger på e-handlarens webbsida, som aktiveras när någon vill handla med ett VISA-kort.[165] Om kortinnehavaren inte är medlem i Verified by VISA märker denne inget utan köpet fortsätter som vanligt. Om kortinnehavaren är medlem ombes han ange sitt lösenord. (Se figur 12.)

[159] http://usa.visa.com/microsites/verified/how_it_works.html
[160] Brodia: http://www.brodia.com/comp_pressRel_010717.htm
[161] http://usa.visa.com/microsites/verified/
[162] Ibid.
[163] http://usa.visa.com/microsites/verified/6_regBegin.html
[164] http://epso.jrc.es/newsletter/vol10/2.html
[165] http://usa.visa.com/business/merchants/verified_index.html



Figur 12. Exempel på användning av Verified by VISA
Källa: Se fotnot [166]

De e-handlare som går med i Verified by VISA blir inte längre ansvariga för bedrägerierkostnader och 'chargebacks'. Kortutfärdarna förlorar sin rätt att ta ut kostnaden för detta, eftersom Verified by VISA kan likställas med en persons underskrift.[167]

Verified by VISA finns, förutom i USA, även i Australien, Indien, New Zeeland, Singapore och Sydkorea.[168] De finska bankerna som är medlemmar i VISA erbjuder sina kortinnehavare och anslutna e-handlare Verified by VISA från och med andra kvartalet år 2002.[169] I Norge har VISA precis börjat med en dialog med e-handlare och kortutfärdare. Enligt tidsplanen ska Verified by VISA introduceras hos ett par norska e-handlare i slutet av år 2002.[170] I april år 2003 måste e-handlare i Europa ha antingen Verified by VISA eller SET (Se avsnitt 1.3, *Avgränsningar*). De e-handlare som inte använder någon av de här teknikerna kommer att få straffavgifter på varje transaktion.[171]

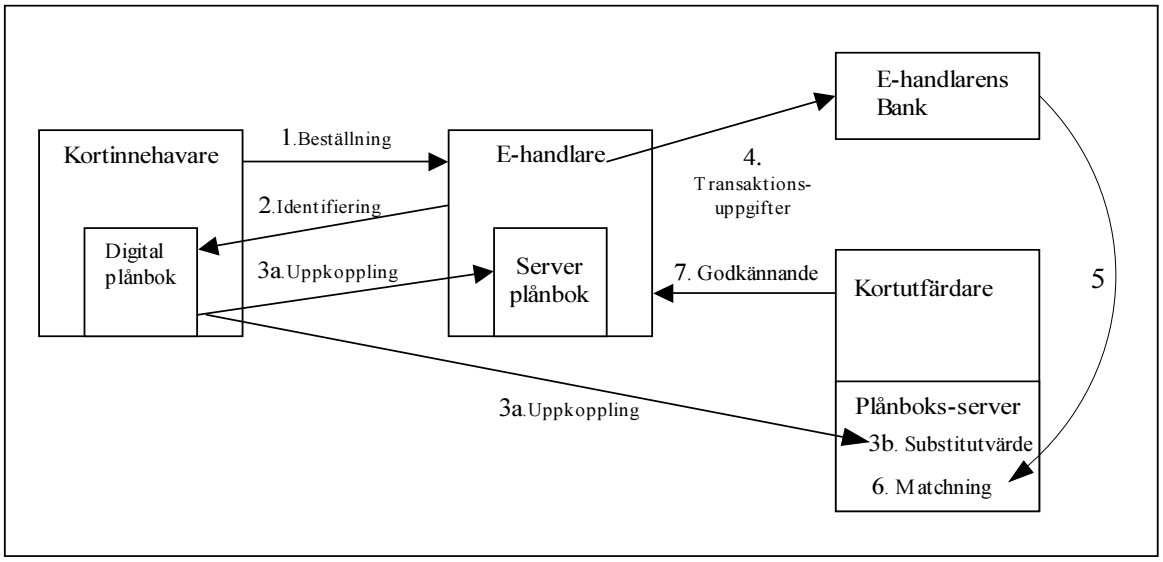
5.2.3.2 SPA från MasterCard

SPA (Secure Payment Authentication) lanserades år 2001 av MasterCard i USA. SPA bygger på ett inbäddat fält på e-handlarens webbplats. Fältet samlar identifieringsdata som genereras av kortutfärdare och kortinnehavare och skapar ett unikt identitetsvärde för kortinnehavaren vid varje transaktion. Detta värde skickas till utfärdaren med en begäran om auktorisering.[172]

Både e-handlaren och kortinnehavaren måste registrera sig för SPA. Kortinnehavaren måste ladda ner en mjukvara i form av en digital plånbok. E-handlaren får något som kallas plånboksserver. Utfärdaren av MasterCard-kortet måste upprätta en server som kan hantera SPA. Servern används för att identifiera kortinnehavarnas identitet med hjälp av till exempel användar-ID och lösenord.[173]

[166] http://usa.visa.com/microsites/verified/how_it_works.html
[167] http://usa.visa.com/business/merchants/verified_index.html
[168] http://www.visa-asia.com/visa_apac/verified/index.shtml
[169] http://www.visaeu.com/press_media/press_releases/finland_12march2002.html
[170] Martin Sivertsen, *VISAs nye passordslösning* (IT-Avisen, 14 december, 2001).
[171] Paradata Systems Inc: http://www.paradata.com/financial/3ds.htm
[172] *Online Card Payments: Fraud Solutions Bid to Win* (Meridien Research, e-Payments, 18 januari, 2001).
[173] Linda Punch, *Defending Online Payments* (Credit Card Management, New York, 2001), 14, 7, s. 42–52.

När en kortinnehavare gör en beställning hos en e-handlare (1) som är med i SPA aktiveras kortinnehavarens digitala plånbok och ber att denne ska identifiera sig (2). Detta sker med ett lösenord som kortinnehavaren fått när han registrerat sig för SPA-tjänsten. Kortinnehavarens plånbok kopplar upp sig mot kortutfärdarens server och e-handlarens plånboksserver (3a) och ett tillfälligt substitutvärde för det riktiga kortnumret skapas (3b). När e-handlarens bank får transaktionsuppgifterna (4) kontrolleras informationen. Om allt är OK skickas uppgifterna till kortutfärdarens plånboksserver (5) där e-handlarens namn matchas med kortinnehavarens digitala plånboksinformation om var kortinnehavaren har handlat (6). Stämmer detta överens godkänner kortutfärdaren transaktionen (7).[174] (Se figur 13.)



Figur 13. En modell över händelseförloppet vid användningen av SPA
Källa: Linda Punch, *Defending Online Payments* (Credit Card Management, New York, 2001)

Enligt MasterCards regler måste e-handlare stå för kostnaden för 'chargebacks' om e-handlaren inte har kortinnehavarens signatur.[175] SPA ger e-handlaren samma skydd som en fysisk signatur från kortinnehavaren. Vid bedrägerier med SPA behöver alltså e-handlaren inte stå för kostnaden för 'chargebacks'.[176] Enligt Stephen W. Orfei på MasterCard sparar även kortutfärdarna pengar med SPA. Om det blir färre 'chargebacks' innebär det mindre kostnader i administration.[177]

5.2.3.3 Private Payments från American Express

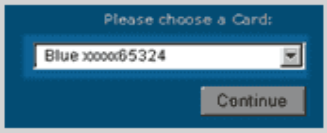
Private Payments är en onlinetjänst för kortinnehavare med American Expresskort som lanserades i september år 2000.[178] Private Payments kan användas på alla e-handelsplatser i USA som tar American Express som betalningsmedel. Vid användandet av den här tekniken går ansvaret för kostnader för bedrägerier över från e-handlaren till kortutfärdaren. Även Private Payments bygger på att ett substitutvärde genereras och detta värde används istället för det riktiga kontonumret. Substitutvärdet har en begränsad giltighetstid på mellan 30 och 67 dagar. Tidsbegränsningen ska förhindra att substitutvärdet missbrukas. Tanken är att kunden ska använda ett nytt substitutvärde för varje transaktion. I och med att substitutvärdet är det enda som e-handlaren får ta del av skyddas kunden.

[174] Linda Punch, *Defending Online Payments* (Credit Card Management, New York, 2001), 14, 7, s. 42–52.
[175] http://www.cardforum.com/html/ccmissue/sep01cov.htm
[176] Linda Punch, *Defending Online Payments* (Credit Card Management, New York, 2001), 14, 7, s. 42–52.
[177] http://www.cardforum.com/html/ccmissue/sep01cov.htm
[178] Lori Enos, *AMEX To Offer 'Disposable' Credit Card Numbers* (Ecommerce Times, 8 september, 2000).

E-handlaren kan inte, till skillnad från med exempelvis SPA, se att det är ett Private Payments-nummer istället för ett riktigt kortnummer. Från att ha haft en inloggningsruta som dyker upp på de anslutna e-handlarnas sida har American Express gått över till att kunderna får gå in på en speciell webbplats och generera sina egna nummer.[179] För att få tillgång till detta måste man ha ett användar-ID och lösenord (se figur 14).

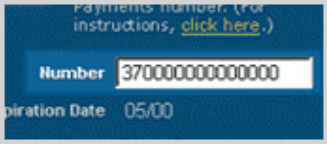
Figur 14. Inloggningsruta på American Express hemsida
Källa: Se fotnot [180]

Lösenord får man genom att fylla i ett formulär. Här måste man ange namn, e-post, kortnummer, födelsedatum samt de fyra sista siffrorna i sitt socialförsäkringsnummer, för att kunna identifiera att det är rätt kortanvändare som vill ha ID och lösenord. När man väl loggat in väljer man det kontokort man vill generera nummer till via en ”drop down” lista.



Figur 15. Ruta för ifyllande av kontokortsnummer
Källa: Se fotnot [181]

Private Payments genererar ett unikt substitutnummer och ett giltighetsdatum, som bara kan användas en gång.



Figur 16. Ruta med genererat substitutvärde
Källa: Se fotnot [182]

Private Payments-numret använder kunden sedan vid handel på Internet. Man kan dubbelklicka på det genererade numret och ”dra” det till e-handlarens fält för kortnummer. Istället för att ange kortets giltighetstid, så anger man giltighetstiden för substitutvärdet.[183] Det krävs ingen mjukvara från e-handlarnas sida, om e-handlaren accepterar American Express kan denne även ta emot Private Payments-nummer. E-handlaren behöver inte längre ta kostnaden om transaktionen är ett bedrägeri. För privatkunder och små företag är tjänsten kostnadsfri. Tjänsten fungerar inte för kort som inte är knutna till en fysisk person, till exempel företagskort. Vidare krävs att kortinnehavaren kan ange en amerikansk leveransadress.[184] På grund av detta kan Private Payments kan endast användas i USA.

[179] http://www.americanexpress.com/privatepayments
[180]https://login.americanexpress.com/sso/default.asp?SSOOP=LOGONPOP&SSOLOGON=LOGONPOP&SSOAPP=PPS&SSOBRAND=EXPRESSNET_PPS&SSOURL=https%3A%2F%2Fwww26%2Eamericanexpress%2Ecom%2Fprivatepayments%2Fppsstart%2Ejsp%3Fsendto%3Dchoose%5Fcard%2Ejsp
[181] http://www26.americanexpress.com/privatepayments/tutorial.jsp
[182] Ibid.
[183] http://www26.americanexpress.com/privatepayments/faq.jsp
[184]https://www.americanexpress.com/pps/en/expressnet/register/RegRegistration?SSOURL=https%3A%2F%2Fwww26%2Eamericanexpress%2Ecom%2Fprivatepayments%2Fppsstart%2Ejsp%3Fsendto%3Dcard%5Fsummary%2Ejsp

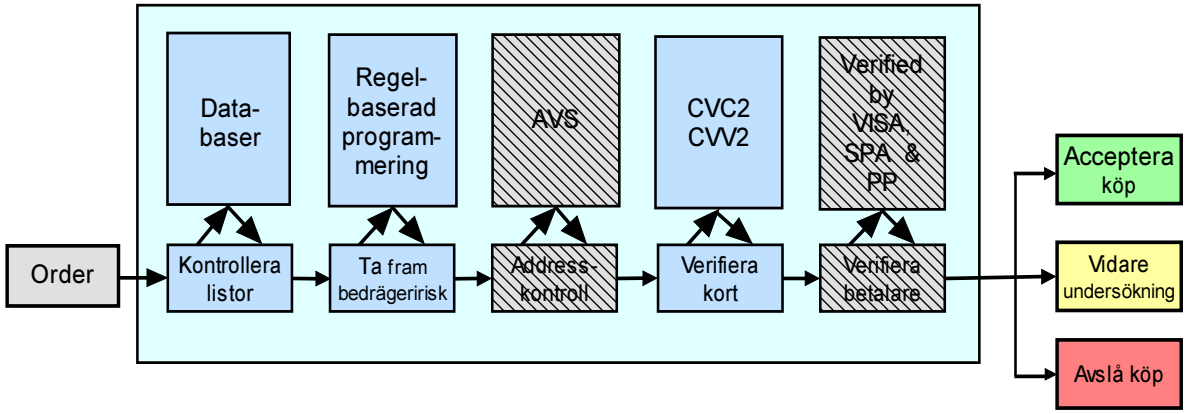
En annan nackdel kan vara att de genererade substitutvärdena har en begränsad giltighetstid. Detta innebär att Private Payments inte lämpar sig vid köp av varor eller tjänster som inte levereras och betalas inom den här tidsperioden. Ett exempel på detta kan vara beställning av en flygbiljett eller hotellreservation, som inte ska betalas inom substitutvärdets giltighetstid. [185]

5.3 Exempel på systemlösningar för bedrägeribekämpning

I följande avsnitt ges exempel från verkligheten på hur tre systemutvecklings- och e-handelsföretags systemlösningar ser ut och fungerar, med inriktning på bedrägerikontroll. Den egenutvecklade översiktsmodellen kommer att användas och anpassas efter de olika systemlösningarnas innehåll för att återknyta till de olika teknikerna redovisade i resultatavsnitten 5.1 och 5.2.

Buyonet[186] är ett e-handels- och systemutvecklingsföretag vars verksamhet startade 1997. Verksamheten går ut på att utveckla, designa samt vara värd för e-handlares Internetbutiker. Allt från att hantera betalningar, skydda mot bedrägerier och kundsupport ingår i systemlösningarna. Förutom att agera värd för andra e-handelsföretag, har Buyonet även egen försäljning av digitala produkter. Huvudkontoret ligger i Sverige, företaget har även kontor i USA. Totalt har Buyonet 50 anställda.

Ett av deras system heter 'the Buyonet Proprietary Anti-Fraud System'. Den första versionen av systemet släpptes i november 1997. Grunden i systemet består av regelbaserad teknologi. Vidare har systemet byggts ut med andra 'scoring'-verktyg under 1998. Implementering av kontroll av verifieringskoder har skett under mars 2002. Buyonet klassificerar de företag som de är värd för efter hur stor bedrägeririsk de har. Därefter anpassas systemlösningen till varje företag för att ge bästa möjliga bedrägeriskydd.



Figur 17. Översiktsmodellen med inriktning på Buyonets e-handelslösning

Bedrägerikontrollen i Buyonets system tar mindre än en sekund. Antalet ärliga kunder som stoppas av systemet uppskattas till cirka 20 %. Vid upptäckt av bedrägerier vidtas inga juridiska åtgärder, däremot lagras information om bedragaren i en speciell databas för att hindra bedragaren vid eventuella nya försök. Buyonet har inget samarbete med några branschorganisationer.

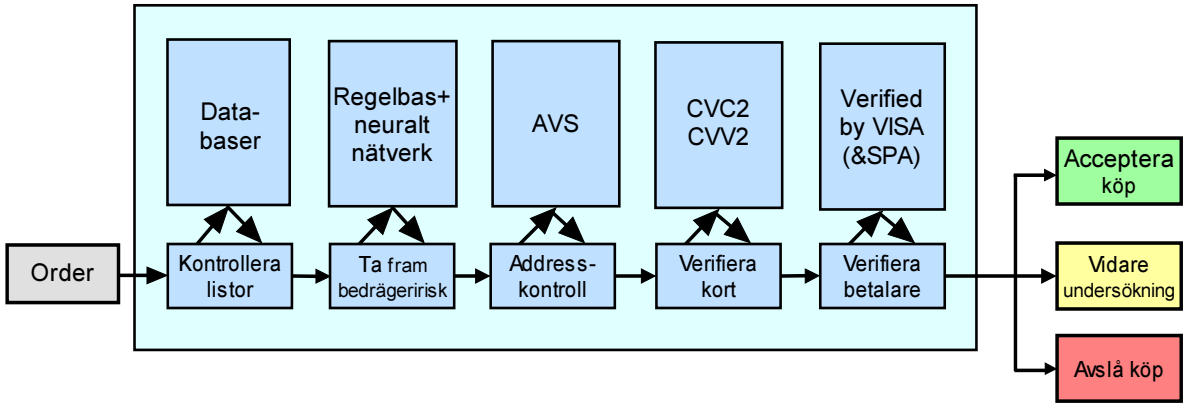
ClearCommerce[187] är ett amerikanskt företag med 230 anställda. ClearCommerce förser e-handlare med automatiserade betalningssystem för Internet. Systemen ska ge e-handlarna möjlighet att integrera sina affärssystem med funktioner som skyddar både e-handlarnas kunder och dem själva

[185] http://www10.americanexpress.com/sif/cda/page/0,1641,4534,00.asp
[186] E-postintervju med Freddy Tengberg, VD för Buyonet.
[187] E-postintervju med Alan Scutt, VD för ClearCommerce i Europa.

från bedrägerier. Huvudkontoret ligger i USA, men de har även kontor i England och Tyskland. Bolaget startade 1995.

Ett system från ClearCommerce heter 'Merchant Engine Payment Software with Risk Management'. Grunden i systemet är ett 'scoring'-verktyg i form av regelbaserad programmering som gör att e-handlare kan förutse resultaten av köpsituationer baserat på förvalda kriterier. Programmet är dynamiskt och kan uppdateras vid behov. Ett artificiellt neuralt nätverk har lagts till i efterhand i september år 2001. Då lades även ytterligare ett 'scoring'-verktyg, 'Fraud Analyzer', till som undersöker mönster i kunders köpbeteende. Den här siffran skickas sedan till det regelbaserade programmet som avgör om köpet ska accepteras, avslås eller skickas vidare för ytterligare kontroll.

Systemet använder sig av AVS för de amerikanska e-handlarna och kontrollerar köparens namn och gatuadress. Systemet använder sig även av kontroll av verifieringskoder, både CVC2 och CVV2, sedan september år 2001. Även 'Payer Authentication'-metoder används; Verified by VISA sedan januari år 2002 och SPA kommer att läggas till senare.



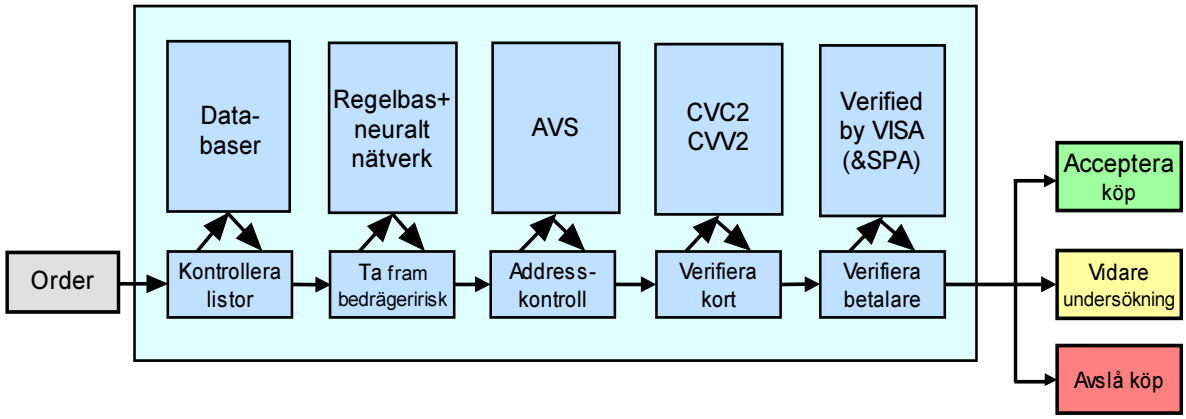
Figur 18. Översiktsmodellen med inriktning mot ClearCommerce's e-handelslösning

ClearCommerce samarbetar med branschorganisationen 'Merchant Fraud Squad'. Systemets bedrägerikontroll tar cirka 5 sekunder.

element 5[188] är ett tyskt företag som förser mjukvaruföretag med en systemlösning för att snabbt, säkert och effektivt sälja produkter på Internet. Systemlösningen ger e-handlare möjlighet att sköta orderhantering, leverans av produkter samt licensiering av produkter helt elektroniskt. Huvud-kontoret ligger i Tyskland. De har även kontor i USA, Storbritannien, Sverige och Frankrike. Bolaget bildades 1996 och har 110 anställda.

Ett av element 5s system heter 'element 5 FraudShield' och är specialiserat på mjukvaruprodukter. Grunden i systemet bestod från början av 'scoring'-verktyg i form av ett artificiellt neuralt nätverk. I juni år 2001 förbättrade man systemet med regelbaserad programmering. Då lades även 'Payer Authentication'-tekniker som Verified by VISA och SPA till. Systemet använder sig sedan oktober år 2001 av AVS för amerikanska e-handlare. Samtliga kunduppgifter kontrolleras, allt från kundens namn till IP-adress. I november år 2001 lades även till kontroll av verifieringskoder som till exempel CVV2 och CVC2.

[188] E-postintervju med Gerrit Schumann, VD på element 5.



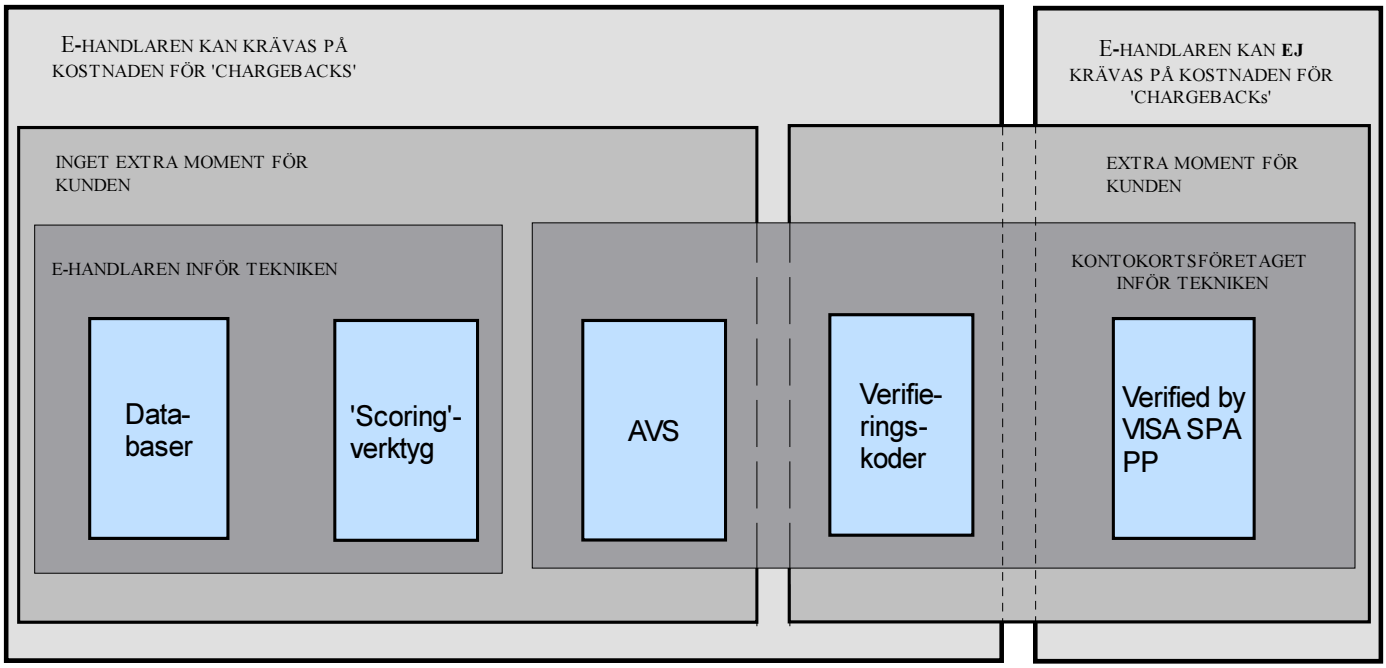
Figur 19. Översiktsmodellen med inriktning mot element 5's e-handelslösning

Bedrägerikontrollen tar 0,5 sekunder och är konstruerat så att inga ärliga kunder stoppas. element 5 delar information om kända bedragare med ett flertal andra företag. De samarbetar även med branschorganisationen SIIA[189].

[189] http://www.siia.net/

5.4 En sammanslagen slutmodell

Slutmodellen bygger på modellen i punktform samt den översiktsmodell vi presenterade i avsnitt 4, *Modeller för redovisning av olika tekniker*. De tre punkterna och modellen har använts vid presentationen av de olika tekniker för bedrägeribekämpning som behandlats tidigare i uppsatsen. Den sammanslagna slutmodellen visar hur ansvaret för bedrägerier fördelas mellan e-handlare och kontokortsföretag/kortutfärdaren. Vår tanke är att detta ska tydliggöra vilka följder de olika teknikerna har för de olika aktörerna och e-handlarnas beroendeställning till kontokortsföretagen. Vi kommer att föra en diskussion, i avsnittet 6.2, *De bedrägeribekämpande teknikerna*, kring var och en av de tekniker som uppsatsen behandlar, med den här modellen som grund.



Figur 20. Slutmodell baserad på modellerna från avsnitt 4, Modeller för redovisning av olika tekniker

Databaser och ’scoring’-verktyg införs av e-handlaren. De här teknikerna innebär inga extra moment för kunden att utföra, vilket kan ses som en fördel för e-handlaren. AVS, som kommer från konto-kortsföretagen, förorsakar inte heller kunderna något extra moment. Dock har e-handlaren fortfarande kvar kostnaden för ’chargeback’ vid ett bedrägeri. Verifieringskoderna, som också kommer från kontokortsföretagen, innebär dock för kunderna ett extra moment. Dessutom har e-handlaren fortfarande kvar kostnaden för ’chargeback’ vid ett bedrägeri. Den enda tekniska lösningen som befriar e-handlaren från ansvaret för ’chargeback’ är ’Payer Authentication’-teknikerna, det vill säga Verified by VISA, SPA och Private Payments. De här teknikerna innebär dock ett antal extra moment för kunden.

6 Diskussion och slutsatser

I det här avsnittet kommer vi att diskutera olika aspekter på de områden i uppsatsen, som vi finner mest intressanta. Bland annat kommer vi att gå djupare in på motsättningarna mellan aktörerna. Vi kommer även att redogöra för våra åsikter angående teknikerna för bedrägeribekämpning. Diskussionsdelen avslutas med ett avsnitt om vidare forskning samt ett avsnitt med självkritik.

6.1 Motsättningarna mellan olika aktörer

Vi menar att dagens e-handlare sitter i en klämd position. Om en e-handlare inte har råd att investera i de bedrägeribekämpande teknikerna som finns, riskerar denne att bli utsatt för stora mängder bedrägerier. Användningen av kontokortsföretagens bedrägeriförebyggande tekniker kan vara kostsam. Det krävs mer pengar och framförallt mer kunskap för att lyckas med en e-handelsverksamhet idag än vad det krävdes för bara ett par år sedan. Man kan säga att en e-handlare måste bedriva krig på alla fronter för att ha en chans att överleva. En front är bedragarna, en annan är kontokortsföretagen och kortutfärdarna som man är så starkt beroende av.

Om e-handlarna vill ha ett handlarkonto för att kunna ta emot kortbetalningar får de helt enkelt acceptera att ta över risken för ’chargebacks’ från kortutfärdaren. Att sedan kontokortsföretagen bestraffar de e-handlare som har många ’chargebacks’ med böter anser vi vara ett utnyttjande av den maktposition som de har, eftersom kontokortsföretagen och kortutfärdarna inte har några direkta kostnader för ’chargebacks’. De här aktörerna har visserligen indirekta kostnader för administrativt arbete genom ’chargeback’-processen, men vi menar att de kostnaderna borde kunna täckas av de ordinarie avgifter för ’chargebacks’ som e-handlarna redan betalar till kontokortsföretagen.[190]

Även systemutvecklingsföretagen påverkas av kontokortsföretagens hårda krav vad det gäller implementeringen av nya tekniker. Systemutvecklingsföretagen måste anpassa sina systemlösningar till de tekniker som kontokortsföretagen har och introducerar. Även e-handlarnas befintliga tekniker måste kunna anpassas till de nya teknikerna som kommer. Det här innebär merarbete för e-handlarna och systemutvecklingsföretagen speciellt om det är en teknik som e-handlaren inte har valt att införa själv utan som kontokortsföretaget kräver ska installeras.

6.2 De bedrägeribekämpande teknikerna

Slutmodellen från avsnitt 5.4, *En sammanslagen slutmodell*, ligger till grund för diskussionen av teknikerna i de efterföljande avsnitten.

I de e-handelslösningar med bedrägeriförebyggande tekniker som vi har tittat närmare på, verkar användningen av databaser vara standard. Det är en ganska logisk teknik eftersom den låter e-handlare lära av tidigare affärshändelser. För bedragare är databaser tyvärr inget större motstånd. Eftersom databaser inte innehåller någon information om en förstagångskund är det troligt att det är just den roll som en bedragare tar. Trots detta är databaser ändå ett bra komplement till andra bedrägeriförebyggande tekniker i en e-handelslösning, på grund av att de stoppar upprepade bedrägerier från inte alltför smarta bedragare.

När det gäller de olika ’scoring’-verktyg som behandlats i uppsatsen har vi sett att de ofta används i kombination med andra tekniker, även andra ’scoring’-verktyg. Det verkar som om utvecklare tänker att: ”De bedrägerier den ena tekniken inte fångar upp tar den andra.”. Regelbaserad programmering och logistikregression är betydligt mindre komplicerade än de artificiella neurala nätverken, eftersom

[190] http://www.dmsontheweb.com/faqs.php

de två förstnämnda bygger på enkel, rak logik och det sistnämnda är mer dynamiskt programmerat och kräver inlärning. Följden blir att de artificiella neurala nätverken blir dyrare, dels på grund av komplexiteten i uppbyggnaden och dels för att det kräver en hel del tid i inlärningsfasen. Hur väl olika 'scoring'-verktyg förhindrar bedrägerier är svårt att säga, eftersom det beror på hur just ett visst system är uppbyggt och hur väl det är anpassat till e-handlarens produkter och kundklientel.

AVS räcker i dagsläget inte långt som ensam bedrägeribekämpande teknik i en e-handelslösning. Det är alldeles för lätt att komma runt kontrollen. Visserligen kan AVS i dag kontrollera mer än bara gatuadressen, men som sagt, det räcker inte. De som verkligen tjänar pengar på AVS är kontokorts-företagen. Självklart har kortutfärdarna kostnader för att underhålla AVS men det känns som om de avgifter AVS drar in är en liten guldkalv för kontokortsföretagen. Många amatörer som försöker sig på bedrägerier stoppas av AVS, men att hitta information på Internet om hur man går runt och lurar AVS är en enkel sak för vem som helst, som vet hur en sökmotor fungerar. Den största fördelen som vi ser det är, att AVS stoppar genererade kontokortsnummer. Detta höjer skyddet för e-handlaren väsentligt. Dock kan det faktum att AVS stoppar så många hederliga kunder ställa till med följd-problem. Det gäller för e-handlaren att vara uppmärksam på problemet och vårda de ärliga kunderna som stoppas. Det kostar visserligen pengar att följa upp de här kunderna, men annars riskerar e-handlaren att tappa kunder som inte kommer tillbaka, och därmed intäkter.

Verifieringskoder är en bra början. Det är, än så länge, valfritt om e-handlaren vill använda verifieringskoder eller inte. Troligtvis skulle en implementering inte röra sig om en större investering, jämfört med vissa andra tekniker, för e-handlaren. Det handlar om ett extra fält i formuläret, som kunden ska fylla i. Även om detta innebär ett extra moment för kunden, anser vi inte att detta är ett så stort steg, så att e-handlaren skulle förlora kunder på det. Sannolikt har kunden kortet framför sig när han fyller i formuläret och att då fylla i några extra siffror tar varken lång tid eller är särskilt krångligt. Eftersom verifieringskoden bygger på en algoritm av kortsiffrorna menar vi att det inte borde vara så svårt att knäcka dem. Det är som mycket annat inom detta område troligtvis bara en tidsfråga.

När det gäller 'Payer Authentication'-tekniker krävs det mer av kundens engagemang än med verifieringskoder. För att man ska gå in på en sida och generera sina egna tillfälliga kortnummer eller ett lösenord krävs kunskap och att kunden vinner något på besväret. Det tar tid och är krångligt för kunden. Det som kunden vinner är en känsla av trygghet; vetskapen att ingen kan handla på kortet utan att kunna koden. Detta gäller dock först när majoriteten av e-handlare är anslutna till 'Payer Authentication'-tekniker. Den som troligen har mest att vinna på den här lösningen är nog ändå e-handlaren eftersom tekniken skickar tillbaka risken vid bedrägerier till kortutfärdaren. Detta kan vara ett stort incitament för e-handlaren att satsa på den här tekniken trots att det innebär ett par extra moment för deras kunder att gå igenom vid ett köp. Frågan är vad kunden har att vinna på att göra sig det extra arbetet, förutom känslan av ökad trygghet. Kunden är trots allt ändå skyddad och får tillbaka sina pengar om något är fel.

Vi antar att VISAs tanke med att kräva att alla e-handlare ska använda Verified by VISA, är att tekniken ska finnas hos alla e-handlare innan de "tvingar" sina kortinnehavare att registrera sig och använda den. Detta skulle innebära ett riskspel för både e-handlare och VISA. Båda parter måste investera en hel del och om Verified by VISA inte får det genomslag som VISA förväntar sig kan det vara bortkastade pengar. VISA har redan ett försök med säkrare betalningar (SET) i bagaget, som anses misslyckat av de flesta.[191]

[191] Johan Rönn, *SET-fiaskot: en miljon kronor per transaktion* (Arbete&IT, 1999).

SPA från MasterCard är den ’Payer Authentication’-teknik som verkar vara mest komplicerad. SPA innebär att kunden är bunden vid en specifik dator, genom mjukvaran, när kunden ska handla. Kunden kan till exempel inte sitta på jobbet och beställa varor. Självklart kan kunden ladda ner mjukvaran på sin arbetsdator, men det kan vara så, att företaget som kunden jobbar på har regler som förbjuder sådant. Det kostar pengar och kompetens, för att e-handlaren ska kunna sköta de olika delarna som krävs vid implementeringen och användningen av SPA.

Att nummer, genererade av American Express Private Payments bara har en viss hållbarhet kan vara både positivt och negativt. Den stora fördelen för e-handlaren att denne inte behöver investera i något; varken i hård eller mjukvara. Dessutom behöver kunden inte vara orolig, för att dennes kontokortsinformation lagras på en dåligt skyddad databas hos e-handlaren. En bedragare kan dessutom bara använda numret en begränsad tid. Nackdelen är att det inte går att beställa varor som ska betalas senare med Private Payments. Vi anser att fördelarna överväger nackdelarna.

En bedragare är naturligtvis inte det minsta intresserad av att registrera sig för något som gör att hans identitet blir avslöjad. Så länge man kan handla på Internet utan att behöva registrera sig kommer troligtvis bedragarna utnyttja detta. För att ’Payer Authentication’-teknikerna ska kunna bli en standard och få ett brett genomslag måste det nog bli obligatoriskt för kunden att registrera sig. En följd av detta kan bli att många kunder tycker att det blir för krångligt och väljer att handla på ett annat sätt än via Internet. Efter ett tag, när alla har vant sig vid en registrering, kan det kanske fungera, men vem ska stå för e-handlarens förlorade inkomster under tiden? Svårigheten med ’Payer Authentication’ är som vi ser det, att få kunderna att börja använda det. Det kan krävas en hel del marknadsföring från kontokortsföretagens sida för nå ut till alla kunder med informationen.

Eftersom det är kortutfärdaren som får stå för risken vid en ’chargeback’ antar vi att ’Payer Authentication’-teknikerna är mycket svåra för bedragare att ta sig runt. Vi anser att kortutfärdarna inte skulle ta på sig bedrägeririsken om inte tekniken betraktas som mycket säker. En annan sak som förvånar oss lite är att VISA och MasterCard valt att utveckla två helt skilda system. De här två företagen har en historia av att samarbeta och det borde vara en fördel för alla om antalet tekniker begränsades. Idag har kunder många olika koder att hålla reda på. Många kunder har även många kort och ytterligare en kod till för varje kort ställer vi oss tveksamma till att kunderna intresserade av.

6.3 Den ideala tekniska lösningen för e-handlarna

I stort sett skulle man kunna säga att den perfekta tekniska lösningen för en e-handlare skulle innebära följande; e-handlaren inför tekniken om och när denne själv vill, tekniken lägger inte till något moment för kunden och att kortutfärdaren får stå för kostnaden för ’chargeback’, om en transaktion visar sig vara ett bedrägeri. Någon sådan teknik finns inte för närvarande

En e-handlare vill självklart använda sig av bedrägeribekämpande tekniker som gör att denne inte behöver betala kostnaderna för ’chargebacks’. Som tidigare nämnts är de enda tekniker som helt befriar e-handlare de kostnaderna är ’Payer Authentication’-teknikerna. De här teknikerna är förhållandevis nya och har än så länge inte fått något större genomslag. Om vi antar att tekniken skulle slå igenom fullt ut, behöver inte e-handlarna system för att stoppa ’chargebacks’. De behöver ett system för att stoppa genererade kontokortsnummer, vilket AVS gör. Detta skulle kunna innebära att systemutvecklingsföretagen förlorar en stor del av sin marknad inom bekämpning av kontokortbedrägerier.

6.4 Framtidsperspektiv

Bedragarna på Internet har ändrat karaktär. Från att ha varit ”mjuka” brottslingar som försökt sig på mindre bedrägerier, till exempel hackare som gör det för prestige och utmaningar, så har bedragarna förvandlats till förhärdade ekonomiska brottslingar[192]. Vi misstänker att framtidens brottslingar kommer att bli ännu hårdare och allt mer skamlösa. Vi kan inte se någon total lösning för kontokorts-bedrägerierna på Internet. Precis som all annan brottslighet kommer den alltid att finnas.

Var går gränsen för hur många olika tekniker e-handlarna ska behöva genom krav från kontokorts-företagen och kortutfärdarna? De olika kontokortsföretagen har sina tekniska lösningar för bedrägeri-bekämpning och e-handlarna får ta smällen. E-handlarna vill kunna ta emot betalningar från olika kontokortsföretag och måste anpassa sig efter deras krav. Ju fler lösningar, desto mer komplicerade systemlösningar och längre behandlingstid blir det per order. Det leder oss fram till en annan aspekt, nämligen tiden som det tar för kunden att gå igenom alla kombinationerna av förebyggande tekniker[193]. Det svåra är att hitta balansgången mellan vad kunden accepterar för kontroller innan han tar sina pengar och handlar någon annanstans och hur stor grad av bedrägerier e-handlaren klarar.

Det bästa för e-handlarna vore om de fick bestämma själva över vilka bedrägeribekämpande tekniker de vill ska ingå i deras e-handelslösningar. Självklart måste det finnas någon form av reglering men idag anser vi att den är för stark och att den kommer från fel aktörer inom branschen. Med risk för att låta kvasikommunistiska, menar vi, att det borde finnas ett internationellt råd som styr vissa sådana regleringar, till exempel vad det gäller standarder. Det borde dessutom inte vara tillåtet för kort-utfärdaren att skriva över risken för bedrägerier till e-handlare. Det är ju faktiskt så, att det är kontokortsföretagen, genom kortutfärdarna, som ska förse e-handlaren med en möjlighet att identifiera kunden. Det har de i och för sig gjort med hjälp av ’Payer Authentication’-teknikerna. Det är dock fortfarande frivilligt för kunderna att använda de här teknikerna. Det är lite samma sak som om en kund inte vill visa legitimation vid ett ’card present’- köp och då kan bli nekad att handla. Vi anser att i dagsläget är dock ’Payer Authentication’-teknikerna den bästa lösningen som finns för kontokort med magnetremsa.

I framtiden kommer smarta kort att lösa många av de problem som finns med kortbedrägerier i olika branscher idag, inte bara inom e-handel. I dagsläget kan smarta kort inte ’skimmas’. Detta kan göra att fler och fler blir villiga att investera i tekniken och infrastrukturen för smarta kort. Men en fråga som vi ställer oss är hur länge det håller. Frågan är nog inte om, någon kan knäcka det smarta kortet, utan snarare när. Så länge smarta kort inte kan ’skimmas’ är detta troligen framtiden. Den befintliga infrastrukturen för kort med magnetremsa är svår att ersätta. Ett skäl till detta är att kostnaden för att byta alla kortläsare kommer att bli betydande. Vem som ska betala införande är svårt att avgöra men e-handlaren kommer troligen att få stå för en stor del av kostnaden. För att smarta kort ska kunna bli ett säkert betalningsmedel vid e-handel måste kunden ha en kortläsare i sin dator. I dagsläget är spridningen av kortläsare för smarta kort starkt begränsad, även i vanliga affärer.

[192] E-postintervju med Alan Scutt, VD för ClearCommerce i Europa.
[193] http://epso.jrc.es/newsletter/vol10/2.html

6.5 Vidare forskning

Det kommer att ta tid innan infrastrukturen för smarta kort är så utvecklad så att man kan anse att det är en standard.[194] Idag kan dock kort med magnetremsa räknas som global standard för kort-betalningar. Om och när smarta kort blir standardbetalning inom e-handel, och även annan handel, är det bara en tidsfråga innan kriminella element knäcker dem också. Då kan det vara intressant att genomföra en undersökning liknande den här, fast med inriktning mot smarta kort istället för mot kort med magnetremsa.

Eftersom förändringar sker hela tiden inom uppsatsens problemområde kan tyngdpunkten på vilka tekniker som kan anses aktuella ändras snabbt. Därför kan det vara intressant att göra en liknande undersökning av bedrägeribekämpande tekniker med jämna mellanrum.

6.6 Självkritik

Vid den första kontakten med våra undersökningsföretag beskrev vi vilken typ av information vi var ute efter. Vi hade hoppats få mer utförlig information från företagen angående deras systemlösningar för bedrägeribekämpning. Trots att företagen inte gav oss all information som vi efterfrågade, har ändå frågeformuläret fyllt sin roll genom att vi kan redovisa hur systemlösningar kan se ut. Om den här undersökningen skulle genomföras av någon annan, med samma metoder och vid samma tidpunkt, skulle deras resultat förmodligen bli mycket likt resultatet i den här uppsatsen. Det finns en möjlighet att personen i fråga skulle kunna få mer utförliga svar från företagen. Vi är också medvetna om att våra tankar och idéer till viss del kan ha blivit färgade av Freddy Tengbergs åsikter under de samtal vi haft med honom. Vi är dock övertygade om att vi varit självrannsakande nog, för att i redovisningen av informationen från företagen ska anses vara gällande.

6.7 Slutsatser i punktform

- Det krävs mer pengar och framförallt mer kunskap för att lyckas med en e-handelsverksamhet idag än vad det krävdes för bara ett par år sedan.
- Att kontokortsföretagen bestraffar de e-handlare som har många ’chargebacks’ med böter anser vi vara ett utnyttjande av deras maktposition.
- Den aktör som tjänar mest på användningen av AVS är kontokortsföretagen.
- AVS stoppar många hederliga kunder och detta ställer till med följdproblem.
- Verifieringskoder kommer troligtvis att knäckas inom en snar framtid.
- Alla aktörer måste använda eller anpassa sig till en bedrägeribekämpande teknik för att den ska ha någon effekt mot bedragare.
- Att bli av med kostanden för ’chargeback’ kan vara ett stort incitament för e-handlaren att satsa på en viss teknik.
- Ju fler tekniker som används, desto mer komplicerade systemlösningar och längre behandlingstid per order.
- Det är svårt att säga hur mycket kontroller och extra moment kunderna är villiga att acceptera.
- Det bör finnas någon form av reglering, men den borde inte komma enbart från kontokortsföretagen..
- Det borde inte vara tillåtet för kortutfärdaren att skriva över kostnaden för ’chargebacks’ till e-handlarna.
- Vi anser att i dagsläget är ’Payer Authentication’-teknikerna den bästa lösningen som finns för kontokort med magnetremsa.

[194] Ken Clark, *In the War on Fraud, a Call for Teamwork* (Chain Store Age, 2000), 76, 11, s. 116–117.

7 Referenser

Böcker:

Arbnor, I. & Bjerke, B. (1994). *Företagsekonomisk metodlära*. Lund: Studentlitteratur.

Backman, J. (1998). *Rapporter och uppsatser*. Lund: Studentlitteratur.

Eriksson, L. T. & Wiedersheim-Paul, F. (1997), *Att utreda, forska och rapportera,* Malmö: Liber Ekonomi.

Holme, I. M. & Krohn Solvang, B. (1997). *Forskningsmetodik. – Om kvalitativa och kvantitativa metoder*. Lund: Studentlitteratur.

Jiming, L. & Yiming, Y. (2001). *E-Commerce Agents*. Berlin: Springer-Verlag.

Mehrotra, K., Mohan, C. K. & Ranka S. (1997) *Elements Of Artificial Neural Networks*. Cambridge: Massachusetts Institute of Technology.

Patel, R. & Davidson, B. (1991). *Forskningsmetodikens grunder*. Lund: Studentlitteratur.

Turban, E. & Lee, J. & King, D. & Chung, H.M. (2000) *Electronic Commerce, A Managerial Perspective.* Prentice-Hall, Inc, New Jersey

Westland, J.C., & Clark, T. H. K. (2000). *Global Electronic Commerce*. Cambridge: Massachusetts Institute of Technology.

Whiteley, D. (2000). *e-Commerce, Strategy, Technologies and Applications*. London: The McGraw-Hill Publishing Company.

Artiklar:

Caldwell, K. (2001). The Public Policy Report. *CommerceNet Newsletter, Vol 3, No. 5.*

Clark, K. (2000). In the War on Fraud, a Call for Teamwork. *Chain Store Age, 76, 11,* 116-117.

Corral, C. B. (1999). On-line Security, Payment Services Aid E-tailers Stung by Fraud. *Discount Store News, 38, 8,* 20-25.

Klemow, J. (1999). Credit Card Transactions via the Internet. *TMA Journal, Atlanta, 1999) 19, 1,* 10-14.

Mandelblit, B. D. (2001). Clicks & crime: The inside story of Internet fraud. *The Security, 38, 9,* 31-32.

Messmer, E. (1999). Credit Crunch for E-comm Wannabes. *Network World, Framingham,16, 22, pp. 64.*

Mehta, R,. & Sivadas, E. (1995). Comparing Response Rates and Response Content in Mail versus Electronic Mail Surveys. *Journal of the Market Research Society, 37, 4,* 429-39.

Murphy, P.A. (2000). The murky world of 'Net chargebacks. *Credit Card Management, 12, 11,* 54-60.

Nyström, A & Kollberg, M & Eliason, J. (1998). *Internethandel i Europa*. , Stockholm:Sveriges Tekniska Attachéer.

O'Sullivan, O. (1999). Egg on its visage. *The USBanker, 109, 6,* 22.

Savage, M. (2000). Online Fraud: New Twist on Old Issue. *Computer Reseller News, 887,* 28.

Punch, L. (2001). Defending Online Payments. *Credit Card Management, 14, 7,* 42-52.

To Build Online Business, Build Trust with Online Merchant Issuers Can Help Fend Off Devastating Fraud Losses. (1999), *Card News, Potomac, 14, 24, p. 1*.

Rapporter och Uppsatser:

Bryant, S. L. (2000) AVS Processing Options, *Virginia University,*
URL http://www.people.virginia.edu/~slb/avs.html

Essler, U. (1999) Electronic Commerce and the organisation of Consumer Trust: The case of electronic payments, Center for Information and Communications Research. *Stockholm School of Economics,*
URL http://www.jrc.es/pages/projects/Essler.htm

Gustavsson, J. (1996), Modeller för betalning på internet, *Högskolan i Örebro*,
URL http://hem.passagen.se/johang/uppsats/uppsats.htm

Höynä, U-K, (1997). Smarta kort - den smartaste lösningen?, *Teldok Info 17*,
URL http://www.teldok.org/pdf/info17.pdf

Malthouse, E.C, (2002), ScoringModels, *Medill School of Journalism, Northwestern University, USA,*
URL http://www.medill.northwestern.edu/faculty/malthouse/ftp/score.pdf

Sandén, W, (1998). Nätet som marknadsplats: De svenska pionjärerna, *KFB och Teldok*, Stockholm,
URL http://www.teldok.org/blurbs/blurb123.htm

Global eCommerce Report 2001. (2001). *Taylor Nelson Sofres Interactive*
URL http://www.tnsofres.com/ger2001/pressoffice/index.cfm

Neural Networks Applied to Direct Marketing. (2000). Sentient Machine Research B.V. Amsterdam, *King's College London,* URLhttp://www.kcl.ac.uk/neuronet/compnies/snnartne.doc

Online Card Payments: Fraud Solutions Bid to Win. (2001, 18 januari). *Meridien Research, e-Payments Vol 4, Report number 3*,
URL http://www.meridien-research.com/doc.asp?docID=423

Merchant Reports and Tools 3.8. (1999) *ClearCommerce*,
URL http://www.mercantec.com/products/download/50downloads/CLRCOMRp.pdf

Internetkällor:

Webbtidningar och andra Internetbaserade nyhetsplatser:
Med Författare:
Armstrong, Illena. (oktober, 2001). Smartcards: Still a Gamble?. *Scmagazine,*
URL http://www.scmagazine.com/scmagazine/2001_10/feature.html

Enos, L. (8 september, 2000). AMEX To Offer 'Disposable' Credit Card Numbers. *Ecommerce Times,* URL http://www.ecommercetimes.com/perl/story/4230.html

Gillmor, S. (2002). Business Pay the Price for Online Credit Fraud*, msn.com*,
URL http://moneycentral.msn.com/articles/smartbuy/scam/1546.asp

Mannix, M. (2002). High-tech Card Fraud Goes on Right Behind Your Back, *usnews.com,*
URL http://www.usnews.com/usnews/nycu/tech/articles/000214/nycu/credit.htm

McWilliams, B. (29 mars, 2001). Welsh Hacker Pleads Guilty to Site Break-ins, *Internetnews.com,*
URL http://www.internetnews.com/dev-news/article/0,,10_728891,00.html

Mello, A. (14 januari, 2002). How Smart Cards Will Revolutionize e-Commerce, *ZDNet News,*
URL http://www.zdnet.com/anchordesk/stories/story/0,10738,2838360,00.html

Mickiewicz, M & Conley, J. (2001). Guide to Online Payment Acceptance, *SitePoint.com,*
URL http://www.ecommercebase.com/article/495

Punch, L. (2001). Building an Online Fortress, *Credit Card Management,*
URL http://www.cardforum.com/html/ccmissue/sep01cov.htm

Rönn, J. (februari, 1999). SET-fiaskot: en miljon kronor per transaktion, *Arbete&IT*,
URL http://www.arbete-it.oval.se/kronika/kronika7.htm

Sandoval, G. (5 oktober, 2001). As Net Fraud Grows, So do E-tailers' fears*, CNET News.com,*
URL http://news.com.com/2100-1017-273977.html?legacy=cnet

Shannon, E. (10 juli, 2000). A New Credit-Card Scam, *Time Europe Magazine Business,*
URL http://www.time.com/time/europe/magazine/2000/0710/creditcard.html

Sivertsen, M. (14 december, 2001). VISAs nye passordslösning, *IT-Avisen,*
URL http://www.itavisen.no/art/1297834.html

Utan författare:
Anatomy of an Internet Credit-Card Scam, (3 april, 2000). *BusinessWeek online,*
URL http://www.businessweek.com/2000/00_14/b3675043.htm

Crackdown och credit-card fraud, (5 november, 2001). *BBC NEWS Business*,
URL http://news.bbc.co.uk/hi/english/business/newsid_1639000/1639178.stm

Identity Theft Tops Consumer Fraud Complaints, Reuters. (23 januari, 2002). *Tech News*,
URL http://www.techtv.com/news/security/story/0,24195,3369333,00.html

Online Banking Statistics – Statistics for General and Online Card Fraud. (2001), *ePayment Resource Center,* URL http://www.epaynews.com/statistics/index.html

Restaurateurs BEWARE! (2001). *Food & Service News,*
URL http://www.restaurantville.com/fsn/fsnplus/skimming.cfm

Shutting-down Credit Card Fraud, (14 augusti, 2001). *Pioneer Petroleums News,* URL
http://www.pioneer.ca/news_detail.asp?strID=39

What is CVV2/CVC2 Code? (2001). *FONBET Corp,*
URL http://www.fonbet.com/cvv2_e.htm

You Can Help Prevent Card Fraud (2000). *E-Advertise,*
URL http://www.e-advertise.com.my/dir/gen_ccfraud.asp

VISA
http://usa.visa.com/business/merchants/verified_index.html
http://usa.visa.com/microsites/verified/
http://usa.visa.com/microsites/verified/6_regBegin.html
http://www.visa-asia.com/visa_apac/verified/index.shtml
http://www.visaeu.com/press_media/press_releases/finland_12march2002.html
http://usa.visa.com/microsites/verified/how_it_works.html
http://www.visa.com

MasterCard
http://www.MasterCard.com
http://www.MasterCardintl.com/about/update/pc_fact.html
http://www.MasterCardintl.com/brand/history.html

American Express
http://www.americanexpress.com
http://www.americanexpress.com/privatepayments
http://www10.americanexpress.com/sif/cda/page/0,1641,4534,00.asp
http://www24.americanexpress.com/sweden/AboutAmex/about_amex_se_fPress.html
http://www26.americanexpress.com/privatepayments/faq.jsp
http://www26.americanexpress.com/privatepayments/tutorial.jsp
http://home5.americanexpress.com/merchant/resources/articles/retail5.asp
https://login.americanexpress.com/sso/default.asp?SSOOP=LOGONPOP&SSOLOGON=LOGONPOP&SSOAPP=PPS&SSOBRAND=EXPRESSNET_PPS&SSOURL=https%3A%2F%2Fwww26%2Eamericanexpress%2Ecom%2Fprivatepayments%2Fppsstart%2Ejsp%3Fsendto%3Dchoose%5Fcard%2Ejsp
https://www.americanexpress.com/pps/en/expressnet/register/RegRegistration?SSOURL=https%3A%2F%2Fwww26%2Eamericanexpress%2Ecom%2Fprivatepayments%2Fppsstart%2Ejsp%3Fsendto%3Dcard%5Fsummary%2Ejsp

EU-källor:
http://epso.jrc.es/newsletter/vol10/2.html
http://europa.eu.int/comm/internal_market/en/ecommerce/chargeback.pdf
http://europa.eu.int/eur-lex/sv/com/cnc/2001/com2001_0011sv01.pdf
http://europa.eu.int/eur-lex/sv/lif/dat/2001/sv_301D0782.html

Systemutvecklingsföretag, e-handelsföretag och andra IT-företag:
Accept Credit Cards Real Time.Com

http://www.acceptcreditcardsrealtime.com/fraud.htm
AriTech Development
http://www.aritechdev.com/ccve/ccve-pic.htm
Brodia
http://www.brodia.com/comp_pressRel_010717.htm
ClearCommerce
http://www.clearcommerce.com/press/articles/wrong_number.html
Clear Card Payment Services
http://www.clearcard.com/support/avs.html
CyberSource:
http://www.cybersource.com/resources/seminars/FraudToolsArchive.ppt
http://www.cybersource.com/fraudreport2001/
http://apps.cybersource.com/library/documentation/product_information_guides/Smart_Authorization_Planning_Guide/html/appA.html
Ernst & Young
http://www.ey.com/global/gcr.nsf/International/International_Home
Informator
http://www.informator.com/Sverige/Allman/Artiklar/Artikel.asp?ArtikelID=9004&ID=245&Aktuellt=45
InternetCash
http://www.internetcash.com/fgo/0,1383,white03,00.html
Keycorp Limited
http://www.keycorp.net/smartcard/What%20will%20drive%20smartcards%20in%20the%20Australian%20marketplace.pdf
Leksell Data
http://www.leksell-data.se/98edis3/set.html
MerchantSeek
http://www.merchantseek.com/glossary.htm
Paradata Systems Inc.
http://www.paradata.com/financial/3ds.htm
http://www.paygateway.com/tech/references/fraud.html
Payment Technologies
http://www.paytech.ru/eng/cvc2.asp
Pennsylvania Maple Syrup
http://www.pennsylvaniamaplesyrup.com/creditcardfraud.htm
RC Knox & Company
http://www.peoples.com/im/cda/rcknox_services/1,,11852,00.html
Wild West Electronics.com
http://www.wildwestelectronics.net/ccv2cidin.html
WorldPay Plc.
http://www.worldpay.com/uk/news/2001/news_fraudadvice.shtml

Branschorganisationer och branschwebbplatser för e-handel:
http://www.aamva.org/Documents/stdBestPracticesMagStripe2dot0.pdf
http://www.aimi.org/technologies/card/magnetic_stripe.htm
http://www.apacs.org.uk
http://www.apacs.org.uk/downloads/skimmingPR.pdf
http://www.cardwatch.org.uk/
http://www.fraud.org.uk/
http://www.iccwbo.org/ccs/news_archives/2000/skimming.asp
http://www.identitytheft.org/

http://www.linuxnet.com/info.html
http://www.merchantfraudsquad.com/Members/membpages/fergerson0101.asp#anchor2
http://www.merchantfraudsquad.com/pages/members.html
http://www.siia.net/

Statliga myndigheters webbplatser:
Storbritannien:
http://www.dwp.gov.uk/publications/dwp/2001/gl33.pdf
http://www.homeoffice.gov.uk/
Sverige:
http://justitie.regeringen.se/pressinfo/pdf/FaktaJu_0107.pdf
USA:
Regulation Z:
URLhttp://www.federalreserve.gov/boarddocs/press/boardacts/2000/20000928/attachment.pdf
What Are Identity Theft and Identity, (US department of Justice, 2000)
URL http://www.usdoj.gov/criminal/fraud/idtheft.html#

Banker och företag inom kontokortsbranschen:
http://atlanticpayment.com/CVV.htm
http://www.dmsontheweb.com/faqs.php
http://www.nordea.fi/SWE/info/news/20020215.ASP?navi=yritysinfo&item=yritysinf
http://swiss-bank-accounts.com/e/faq/CVV2.html

Alla webbadresser är kontrollerade 2002-05-22

E-postintervjuer med följande personer:
Freddy Tengberg, VD för Buyonet. http://www.buyonet.com
Alan Scutt, VD för ClearCommerce i Europa. http://www.clearcommerce.com
Gerrit Schumann, VD för element 5. http://www.element5.com

8 Bilaga: Frågeformulär

Department of Informatics
School of Economics and Commercial Law
Gothenburg University

Questionnaire for Research on Credit Card Fraud in E-commerce

Introduction

This questionnaire is part of the foundation of a research report on credit card fraud in e-commerce. The research is for a Master research report at the Department of Informatics at the School of Economics and commercial Law at the Gothenburg University in Sweden. The results of this research will be distributed to the participating companies electronically or by mail according to your request. We expect to be finished with the analysis of the questionnaire during May 2002.

The questions can be answered directly in the document and the completed questionnaire can be sent either by email to: s99liv@student.informatik.gu.se or by mail to: Anna Segerstad, Stuartsg.4, 41260, Gothenburg, Sweden. Please, return the completed questionnaire **before March 22 2002.** If any answers from the questionnaire are unclear, we may get back to you. If you have any questions, please contact us for further information.

Thank you for your participation!

Best regards,

Liv Bryngelsson, +46 707 300 777, s99liv@student.informatik.gu.se
Anna Segerstad, +46 736 94 94 21, s99seger@student.informatik.gu.se

About Your System Solution:

The following questions concern functions for fraud prevention in and general information about your e-commerce solutions for digital products. ***Chose one of your solutions!***

1. What is the name of the system solution you have chosen to represent in this research?
   Answer:

2. When was your system solution released? (Year and month if possible)
   Answer:

3. Does your system solution accept anonymous email addresses like Yahoo or Hotmail?
   Answer:

4. Does your system solution use AVS or any other address verification functions? (If answer is no, go to question number 8.)
   Answer:

5. If AVS or similar is used, what kind of information is verified? (**Mark** with X)
   First name:
   Last name:
   Postal address:
   Zip-code:
   Country:
   IP-address:
   Other (please, specify):

6. When was AVS added to your system solution? (Year and month if possible)
   Answer:

7. Does your system solution use any Card Verification Methods like for instance CVV2 or CVC2? (If answer is no, go to question number 9.)
   Answer:

8. When was the Card Verification Method added to the system solution? (Year and month if possible)
   Answer:

9. Does your system solution use any Payer Authentication Methods like for instance Verified by VISA or SPA by MasterCard? (If answer is no, go to question number 11.)
   Answer:

10. When was the Payer Authentication Method added to the system solution? (Year and month if possible)
    Answer:

11. Does your system solution use any Rule-Based technology? If so, what kind? (If answer is no, go to question number 13)
    Answer:

12. When was the Rule-Based technology added to the system solution? (Year and month if possible)
    Answer:

13. Does your system solution use Neural Computing? If so, what kind? (If answer is no, go to question number 17.)
    Answer:

14. When was the Neural Computing added to the system solution? (Year and month if possible)
    Answer:

15. Does your system solution use any other Fraud Scoring tools? If so, what kind? (If answer is no, go to question number 15.)
    Answer:

16. When was the Fraud Scoring tools added to the system solution? (Year and month if possible)
    Answer:

17. Does your system solution use other functions for fraud prevention not listed above? If so, what kind?
    Answer:

18. If so, what functions and when were they added to the system solution?
    Answer:

19. Are you planning to implement any new functions in your system solution? If so, when and of what kind?
    Answer:

20. What is the total time for fraud screening in your system solution? (From when customer submits order until getting message about order accepted or not)
    Answer:

21. How many non-fraudulent customers are stopped the fraud screening process of your system solution?
    Answer:

About Credit Card Fraud:

The following questions concern how credit card fraud has affected the system solution you have chosen for this research. Some questions concern your policies on credit card fraud.

22. What are your routines concerning handling detected credit card frauds? For instance, are any legal actions taken or do you involve non-profit fraud prevention organisations?
    Answer:

23. Do you cooperate with any industry organisations? (For example, by sharing fraudulent customer information)
    Answer:

24. From which countries do you get the most fraudulent orders? (Please, name the top countries and percentage of total credit card fraud)
    Answer:

25. How do you determine which country a fraudulent order comes from?
    Answer:

26. What is your limit for how far you intend to prevent credit card fraud? (For instance, in terms of percentage of revenue or transactions)
    Answer:

27. What is the credit card fraud rate for your system solution today, in percentage of revenue?
    Answer:

28. What is the credit card fraud rate for your system solution today, in percentage of transactions?
    Answer:

29. From your founding year, how has the credit card fraud rate changed in terms of percentage of revenue? (Please, list per year)
    Answer:

30. From your founding year, how has the credit card fraud rate changed in terms of percentage of transactions? (Please, list per year)
    Answer:

About your company:

The following questions concern general information about your company.

31. What year was your company founded?
    Answer:

32. How many employees are there?
    Answer:

33. In which countries are you established and where is your head office?
    Answer:

36. How are your sales for digital products divided on countries?
    Nationally: %
    Europe: %
    USA: %
    Other countries: %

If there are any other questions or information you think should be included in this questionnaire, please let us know.

If you have any questions do not hesitate to contact us per email or by phone according to the information in the introduction.

Thank you for your participation!

Best regards,

Liv and Anna