



# BLÅSNINGEN

Det började med ett märkligt kontoutdrag och en försvunnen struntsumma.

Två månader senare var tiotusentals svenskar tvungna att byta bankkort, miljontals kronor var på vift och en brittisk säkerhetsexpert flögs till Stockholm för att lösa den största kortsvindeln i svensk historia. Här är berättelsen som din bank inte vill att du ska läsa.

TEXT: DANIEL OLSSON ILLUSTRATIONER OCH GRAFIK: RICKARD FRANK

**J**esper Öhnstedt visste att hans kompanjon aldrig skulle stänga av sin mobiltelefon. Det stred mot Mattias Erikssons natur. Mattias var den där typen som inte protesterade om så kunderna väckte honom klockan tre på morgonen, för att fem minuter senare slänga sig in i en taxi och be att få bli körd till någon nattklubb som behövde få igång kassan inför sista beställningen.

Men med tanke på vad som hänt de senaste dagarna visste Jesper inte längre vad han skulle tro om sin affärspartner.

Bankernas privatutredare från England hade varit uppe på kontoret dagen innan och lämnat dem med ett ultimatum. Fram till dess hade han pratat om allmänna säkerhetsbrister i det betalssystem som Jesper och Mattias utvecklat i sitt kassaföretag Alphacash. Nu var tonen betydligt skarpare. Utredaren anklagade dem för brott, för att tillsammans med en dömd kortbedragare ha iscensatt den största kortkortshärvan i svensk historia.

– Vi vet ju att det är någon av er, gräv fram det nu, pressade engelsmannen.

Jesper och Mattias fick ett dygn på sig att ta fram den skyldige, annars skulle polisen kopplas in.

Jesper hade utredarens ord i huvudet när han gjorde ytterligare ett försök att nå Mattias. Men inte ens telefonsvararen gick igång. Telefonen var avstängd. Det var då han förstod att hans kompanjon och den drivande kraften bakom Alphacash hade flytt landet.

Jesper ringde till polisen.

**D**et hela började ganska precis två månader tidigare. Det var den stora lönedagen efter jul- och nyårshelgerna och ett tunt lager nyfallen snö gnistrade på trottoaren utanför den nyligen nedlagda Tempobutiken på Djurö. Stora pappkassar satt upptejade på insidan av skyltfönstren, men förbipasserande kunde ändå ana skenet från tända lysrör genom den tunna pappen.

Klockan hade hunnit bli kvart över åtta på kvällen när en man slog sig ned vid en av kassorna och

började knappa in sifferkoder i betalkortsläsaren. Först sexton siffror för kortnumret, därefter fyra för sista giltighetsdatum och slutligen köpesumman efter eget huvud.

En sista knapptryckning och kortterminalen sände iväg en köporder över telefonlinjen. Proceduren upprepades om och om igen. Fingrarna rörde sig över knappatsen.

Innan bankernas säkerhetssystem hann reagera hade mannen i kassan styrt över 1,2 miljoner kronor från 107 bankkonton till butikens postgiro.

Det tog exakt 59 minuter.

Några dagar senare loggade konsulten Mattias Öman in på sin internetbank via datorn hemma på Lidingö. Nästan sextusen kronor saknades på lönekotot. Hans ögon sökte sig över kontoutdraget och fann att någon, samma dag som februarilönen kom in, hade gjort tre köp med allt större summor.

Alla köp var gjorda i en liten Tempobutik ute på Djurö.

»Tempo, finns den kedjan kvar?« var Mattias Ömans första tanke.

Även om det bara var knappt trettio minuters bilväg till det idylliska skärgårdssamhället nordost om Stockholm, var han säker på att han inte varit där under någon av de senaste dagarna.

Mystiken tätnade när Mattias Öman kom till jobbet dagen därpå och fick veta att tre av hans arbetskamrater på samma firma inom telekombranschen hade drabbats av samma sak. En av arbetskamraterna ringde upp Tempobutiken för att reda ut vad som hänt.

Kvinnan som svarade berättade att hon blivit kontaktad av fler drabbade, men att butiken var stängd sedan flera veckor och att det måste röra sig om någon form av bedrägeri. Hon kunde också berätta att hennes arbetskamrater inte fått sina löner utbetalda och att butikens ägare var spårlöst försvunnen.

Butiken låg inrymd i botten av en trevåningsfastighet från 60-talet med många äldre hyresgäster som hade hoppats att den nya ägaren skulle bringa ordning och reda på deras närbutik.

Den nya ägaren presenterade sig för de anställda som Jean Naaoum. Han var en välklädd ung man som talade engelska med amerikansk accent. Han fick betala en krona för butiken mot att han också tog över den gamla ägarens obetalda skatter och

leverantörsskulder. I gengäld var alla butiksinventarier och ett betalkortsavtal hans.

Någon större ordning hann det inte bli på närbutikens. De äldre hyresgästerna på våningarna ovanför kunde istället storögt titta ut genom köksfönstren på eftermiddagarna och se den nya butiksföreståndaren komma till jobbet i limousin, för att andra dagar parkera en exklusiv mörkblå Jaguar framför butiken.

Jean Naaoum själv pratade gärna om sina båtaffärer i utlandet och några av dem han mötte skulle senare dra sig till minnes det ologiska i att den proppklädda mannen sade sig bo på Hotell Hilton i centrala Stockholm, samtidigt som de själva tyckte sig ana att han tillbringade de flesta nätterna på soffan inne i den mögeldrabbade livsmedelsbutikens kontor.

Dagen efter lönedagen var ägaren borta. Med sig tog han kassaterminalen och hårddisken till butikens dator.

**P**å bedrägerirotelns våning högt upp i polis-huset på Kungsholmen i Stockholm var Jean Naaoum ett välbekant namn. Två polisinspektörer hade jagat honom i ett halvår, men hela tiden varit steget efter.

De hade lyssnat till förtvivlade ungdomar som lagt sina sparade pengar på förskottshyror för en ledig etta med kokvrå på Södermalm som aldrig fanns. De hade besökt ekande tomma företagslokaler som tagits över av något av Jean Naaoums bolag med postbox på Strandvägen, för att sedan plundras på inventarier för miljontals kronor.

En gammal flickvän kände honom under det Gudfadern-inspirerade namnet Ramone Carleone, medan medierna hade döpt honom till »Stureplansbedragaren« på grund av hans extravaganta utsvävningar i Stockholms krogcentrum. Under namnet Elias Malki var han dömd för kontokortsbedrägerier, sedan han under ett par intensiva veckor 2003 levte som en kung på Norrköpings innekrogar; bjudit generöst på champagne och gjort stora kontantuttag med egentillverkade kontokort med falsk information inpräntad i magnetremsan.

Den man som verkliga hette Jean Naaoum, upptäckte polisutredarna snart, var en österrisk medborgare som avlidit flera år tidigare.

Efter några veckor ringde Swedbanks

säkerhetsavdelning till Bedrägeriroteln och berättade att man spårat samtliga kortnummer som knappats in i kassan på Djurö till en lunchrestaurang i Hallonbergen, Beirut By Night. Många av restaurangens lunchgäster arbetade inom telekomindustrin i det närliggande Kistaområdet och korten de betalade sina notor med var ofta kopplade till företagskonton med hög eller ingen övre uttagsgräns.

För ägaren till Beirut By Night var det hela ett mysterium. Han litade på sina anställda, och hade dessutom lagt mycket pengar på ett helt nytt kassasystem från ett relativt nystartat kassaföretag i Norrköping.

Hur kunde hans kunders kortnummer hamna hos en ökad bedragare?

**K**assaföretaget Alphacash kontor låg inhyst i en liten men vacker trerumslägenhet högt upp på tredje våningen i en sliten tegelfastighet på Trädgårdsgatan i centrala Norrköping. Det hade högt i tak, med stuckaturer och stora fönster mot gatan där de öststatsliknande spårvagnarna då och då slamrade förbi.

Hade det inte varit för alla gamla lunchkartonger, urdruckna pet-flaskor och svarta soppåsar hade det kunnat röra sig om vilket litet innerstadskontor som helst. Nu påminde det mer om en ungarlyslysa.

Här satt Jesper Öhnstedt och den tredje delägaren Jonas Petersson vid var sin PC-dator och utvecklade Alphacash programvara, medan Mattias Eriksson åkte runt till kunder i firmans Volvo. De var alla i trettioårsåldern.

Mattias var den naturliga företrädaren för företaget. Det var också han som stod som kontaktperson när registreringshandlingarna skickades in till bolagsverket i maj 2005. Då hade han flera bolag inom databranschen bakom sig. Några år tidigare hade han drivit en liten datorbutik i Norrköping tillsammans med en barndomsvän från Krokek. Men när han insåg att han tjänade mer pengar på att installera nätverk och utföra andra sysslor på konsultbasis lade han ned butiken.

– Alla säljer datorer i dag i alla fall, resonerade han.

På en restaurangägares inrådan fick han upp ögonen för kassaterminalbranschen. Tidpunkten var precis rätt. Där fanns mycket pengar att hämta.

Med allt hårdare redovisningskrav från skattemyndigheten och med kortbetalningarnas verkliga genombrott behövde gamla kassaregister ersättas av moderna terminaler. Och flera kassaterminaler på marknaden bestod av vanliga PC-system som Mattias Eriksson redan var van att arbeta med.

Han började serva kassasystem i Norrköpings krogvärld och blev snart känd som en både effektiv och kompromissvillig datatekniker.

Genom ett konsultuppdrag för det göteborgsbaserade företaget POS One kom han i kontakt med företagaren Håkan Tegelberg, en verklig veteran inom kassabranschen.

## »En man som inte hade lämnat Norrköping på flera månader, men som dragit sitt kort på en av innekrogarna i stan, upptäckte att pengar togs ut från hans konto – i USA.«

Håkan hade sålt kassaregister i trettio år och började tröttna på alla klagomål från kunder med krånglande terminaler. I Mattias Eriksson såg han en driven person som delade hans planer att utveckla enklare programvara, med mindre krångel.

Håkan Tegelberg anställde Mattias Eriksson och hans två programmeringskunniga vänner Jonas Petersson och Jesper Öhnstedt. Håkan Tegelberg såg sig som pappa för projektet, och stod för finansieringen mot att han någon gång i framtiden vid en eventuell försäljning skulle få en stor del av pengarna.

Framtiden såg ljus ut.

För att få koppla kassaterminalerna till kortsystemet slöts ett avtal med Strålfors, ett av de servicebolag som agerar länk mellan banker,

butiker och kortföretag. Därmed var Alphacash godkända som en i raden av leverantörer av kassaterminaler till restauranger och butiker – och officiellt insläppta bakom murarna till det digitala betalningssystemet.

I Alphacash utvecklades Mattias Eriksson till en verklig säljmaskin. Han levde för jobbet och beskrivs som en naturbegåvning, en säljare av den gamla skolan där det räckte med ett handslag, sedan var allt okej.

Hans arbete kretsade kring restauranger och krogar. Såldes han inte kassaterminaler för Alphacash, kunde han ställa upp som entrévärd eller diskjockey. Därmed kom han också i kontakt med de mer ljusskygga sidorna av krogvärlden, som finns också i en mellanstor stad som Norrköping.

En dag nämnde han för Jonas att han hjälpt den lokala MC-klubben Top Hat MC att installera ett krypteringsprogram på klubbens datorer.

– Var det så väldans smart? frågade Jonas, väl medveten om att klubben aspirerade på

att bli Hells Angels nästa avdelning i Norrköping.

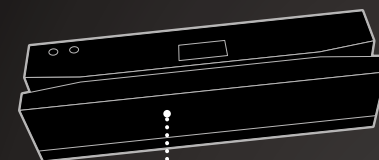
Mattias Eriksson ryckte på axlarna, och menade att han bara hjälpte några killar han träffat på krogen.

När Jonas träffade en tjej i Thailand och blev allt mindre intresserad av att dra runt på krogen, gled de båda vännerna ifrån varandra. Mattias sökte sig till nytt umgänge på de mer utpräglade ineställena i Norrköping, där han beskrivs som en person som sprang runt med tjocka sedelbuntar i fickan och som kunde spendera tusentals kronor under en kväll.

För dem som ville lyssna berättade han om sin dröm att lämna stressen i Sverige. Han tänkte inte bli som sin pappa, som satt hemma i lägenheten i Krokek, drabbad av hjärtproblem redan innan han fyllde fyrtio. Det var inte värt det. Istället skulle Mattias Eriksson packa väskorna en dag, och flytta till Brasilien.

## VAD ÄR SKIMNING?

Skimming innebär att informationen i ett kontokorts magnetremsa kopieras. Därefter överförs den antingen till ett nytt kort, eller utnyttjas för köp per Internet, telefon eller postorder.

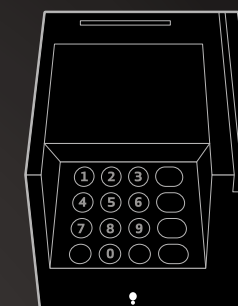


### MINISKIMMER

Så diskret att en servitör eller butiksanställd kan gömma den i handen, och kopiera ditt kort utan att du ser det. Då läsaren är så lik utrustningen man använder för att rengöra kreditkort, är en annan variant att du får ditt kort tvättat – men i själva verket kopierat – medan du ser på.

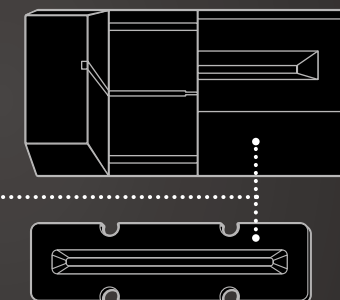
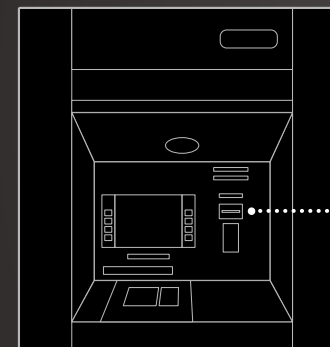
### UTTAGSAUTOMATSKIMMER

Genom att fästa en kopieringsstillsats framför bankomatens kortläsare, eller montera på en komplett falsk front, kan bedragare stjäla din kontoinformation när du tar ut pengar. Kombinerar ofta med en spionkamera som registrerar din kod.



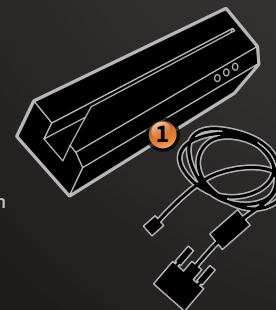
### BUTIKSSKIMMER

Under ett inbrott placeras kopieringsutrustning inne i butikens egen kortläsare, eller en helt ny, specialpreparerad, kortterminal. Vid ett nytt inbrott hämtas utrustningen och informationen hem.



## SÅ SKAPAS FALSKA KREDITKORT

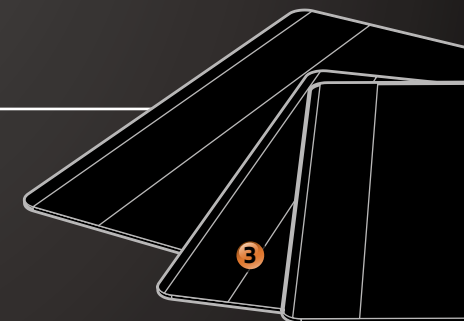
1. Magnetkorts-skrivare med USB-anslutning kostar några hundra dollar, och finns att beställa via internet från tillverkare i Kina.



2. Programvaran är endast 2 Mb stor, vilket gör att bedragaren kan ladda ner den från Internet vid behov och inte behöver spara den på den egna hårddisken.



3. Informationen kan skrivas antingen på vilket gammalt betal- eller medlemskort med magnetremsa som helst, eller på fabriksnya kort med remsa.



I november 2006 köpte han en tomt i området Maxaranguape, ett fiskesamhälle med tiotusen invånare, drygt två mil norr om den stora turistmetropolen Natal och inte långt ifrån fotbollsstjärnan David Beckhams och den inhemske formel ett-stjärnan Ruben Barrichellos gemensamma lyxresort Cabo São Roque.

Hela kustresan var fylld av stora spekulationsprojekt. Med norska oljepengar och under den norska »*selfmade*« finansmannen Svein-Erik Bakkes ledning skulle det idylliska fiskesamhället inom tio år vara förvandlat till världens största semesterby med 5 000 lägenheter, åtta hotell och tre golfbanor.

En fantastisk dröm och slutmålet för ett hårt arbetsliv enligt vissa. Ett vansinnesprojekt enligt andra.

Det fanns ju inte ens en asfalterad väg från Natal till Maxaranguape.

Tre veckor efter att Mattias Eriksson köpt sin tomt begick Svein-Erik Bakke självmord och hela högriskprojektet sattes i gungning.

Det fick inte Mattias att sluta drömma.

Så gott som dagligen fick vännerna höra om fördelarna med att lämna Sverige. Mattias Eriksson skulle sticka när det arkitektritade huset var färdigbyggt, om kanske fem år. Han skulle sälja bolaget, och sedan leva på avkastningen.

Hur lätt var inte allt därnere!

Medan polisen jagade »Jean Naaoum« för kortbedrägerierna på Djurö uppmärksammades de svenska bankerna på allt fler obehöriga transaktioner. I månadsskiftet januari-februari 2007 drabbades en av Handelsbankens kunder av ett obehörigt uttag på 9 074 kronor. Ännu en gång kunde det spåras till ett kort som använts på Beirut By Night, men den här gången gjordes inte uttaget på en butik i Stockholms skärgård, utan på en ögrupp nästan tusen mil därifrån: Filippinerna.

Nu började rapporterna dessutom strömma in om skumma uttag från kort som aldrig hade varit i närheten av restaurangen i Hallonbergen.

Fem kort som räckts över till personalen på en stor nattklubb i Borås användes för kortköp för sammanlagt 161 000 kronor. Även den gången gjordes uttagen på Filippinerna, men också i Thailand.

En man som inte hade lämnat Norrköping på flera månader, men som dragit sitt kort på en av innekrogarna i stan, upptäckte att pengar togs ut från hans konto – i USA.

Alla storbanker var drabbade, utan urskiljning.

Någonstans i det digitala betalningssystemet fanns uppenbarligen en lucka. Det enda bankerna kunde göra innan den hade tätats var att ersätta kunderna med de förlorade beloppen, och spärra kortnumren i den takt bedrägerierna uppdagades.

Varje dag görs över tre miljoner transaktioner med svenska bank- och kreditkort. Det innebär att enorma värden förflyttas inom kortsystemet, värden som tidigare fanns uppdelade i var mans plånbok i form av sedlar och mynt.

För banker och handlare finns det mycket att tjäna på den här övergången – så sent som i början av 90-talet var tjugofem procent av bankernas kostnader kopplade till hanteringen av kontanter. Betalkorten har inneburit färre butiksran, färre kostsamma penningtransporter och ökade skatteintäkter för staten i och med att det blivit svårare att betala svart för varor och tjänster. För varje kortköp tjänar dessutom systemets olika aktörer pengar i form av avgifter.

I takt med övergången till kort har de digitala säkerhetskraven ökat. Det måste gå att lita på systemet – annars påverkas hela samhällsekonomin.

Alla svenska banker håller sig därför med egna säkerhetsavdelningar som dygnet runt, sju dagar i veckan, med hjälp av sofistikerade system skannar av samtliga korttransaktioner i jakt på händelser som skiljer sig från det normala. Om någon handlar mjölk på Ica i Tranemo för att en halvtimme senare dra samma kort hos en taxichaufför i Johannesburg, finns det system som får ett meddelande att omedelbart dyka upp på dataskärmarna inne på bankernas säkerhetsavdelningar. Enligt företaget Secana, som bland annat anlitas av SEB för skanning av kundernas köpbeteenden, upptäckts 86 procent av alla kortbedrägerier genom den typen av automatiserade kontroller.

Det som nu drabbade de svenska bankerna antydde problem av mycket större dignitet. Och för åtminstone några av de inblandade experterna måste det inträffa ha gett en obehaglig känsla av déjà vu.

Västsvensken Magnus Jakobsson var 25 år gammal när han 1999 trädde in på den internationella kortbedragarscenen.

Han hade begått en del småbrott tidigare – några inbrott i skolor och kontorslokaler tillsammans med kompisar, enklare kortbedrägerier, innehav av nio högexplosiva sprängkapslar »för att tillverka en nyårsmällare«. I de lokala medierna var han omskriven som »radiomarodören« som byggde om sin radioutrustning för att gå in och sända på polisens frekvenser.

»Jag ville bara retas lite«, sade den unge mannen under en rättegång där han även beskrev sitt stora intresse för att plocka isär och bygga ihop tekniska apparater.

När han sommaren 1999 kom i kontakt med en ryss vid namn Andrej Golov tog småfyllaren ett stort kliv rakt in i grov organiserad brottslighet. Golov var säkerhetschef vid den ryska storbanken Alfa Bank/Union Card, och beskrivs som ett matematiskt geni som fallit för frestelsen att tjäna stora och snabba pengar.

Genom sitt arbete hade han full tillgång till bankens datasystem, inklusive krypteringsnycklar och servrar som hanterade elektronisk trafik för samtliga utländska kort som stacks in i uttagsautomater runt om i Ryssland. Andrej Golov tog sig in i systemet och stal hundratals kortnummer med tillhörande pinkoder.

Men han behövde någon som kunde föra över kortinformationen till nya plastkort, och som kunde ta risken att plocka ut pengarna. Gärna långt bort från Ryssland.

Andrej Golov blev imponerad av Magnus Jakobssons kunskaper och erbjöd honom kortinformationen i utbyte mot att han själv fick 60 procent av allt som plockades ut ur automaterna. Magnus Jakobsson godkände villkoren och fick tjugotill-trettio tusen kortnummer med tillhörande pinkoder skickade till sig.

Svensken tillverkade vita, hemmagjorda betalkort med den fyrsiffriga koden inskriven i plasten. Under ett drygt år plockade Magnus Jakobsson och personer som han anlidade ut minst tio miljoner kronor ur uttagsautomater över hela Västeuropa. Sverige, särskilt Göteborgsområdet, var extra hårt drabbat.

Det dröjde mer än ett år innan polisen lyckades stoppa det som då beskrevs som den största internationella kortbedrägerihärvan någonsin. Flera av personerna som greps med Magnus Jakobssons plastkort var medlemmar i det nybildade kriminella gänget Original Gangsters. Hösten 2001 dömdes Magnus Jakobsson till fem och ett halvt års fängelse

## »Ju längre mötet fortgick, desto mer insåg Jonas och Jesper att många av frågorna handlade om sådant som bara Mattias Eriksson kunde svara på. Men han var i Brasilien.«

för grova organiserade kortbedrägerier, och för att ha skaffat fram 21 pistoler åt personer i den kriminella gängmiljön.

Nu användes liknande bedrägerimetoder igen. Än en gång stod Sverige i centrum.

I månadsskiftet februari och mars 2007 flögs i största hemlighet europachefen för det brittiska säkerhetsföretaget Cybertrusts avdelning för kriminaltekniska utredningar till Stockholm för att inleda en privat undersökning åt de fyra svenska storbankerna.

Cybertrusts utredare kom fram till att det inte var de enskilda restaurangerna som var felkällan i den växande svenska korthärvan, utan restaurangernas kassasystem. Alla drabbade restauranger hade kassor med integrerade kortläsare som de inhandlat från ett Norrköpingsbolag.

Alphacash var en av de mindre aktörerna inom kassabranschen med drygt 120 sålda kassor utspridda på ett åttiotal restauranger i framför allt Göteborgs- och Norrköpingsområdet, men det räckte för att nästan 200 000 kortkunder haft möjlighet att dra sitt kort genom terminalerna.

Cybertrusts utredare fann att Alphacash kassaterminaler i strid mot alla branschens regler sparade informationen från alla kort som dragits i restaurangerna. Den låg kvar okrypterad i terminalernas minne, och kunde när som helst tankas

## »Under kvällen lade Mattias Eriksson plötsligt upp en tjock bunt med sedlar på vardagsrumsbordet inför Håkan Tegelberg och hans familj. Det var närmare 200 000 kronor.«

över till ett USB-minne eller brännas över till en CD-skiva. Det gjorde Alphacash kassaterminaler till stora skimmingstrutrustningar fyllda med värdefull kortinformation.

Samtidigt hittade utredaren ett fjärrstyrningsprogram i kassaterminalerna som tillät personer att ta sig in i terminalerna och hämta hem information varhelst ifrån.

Utredaren från Cybertrust rapporterade till sina uppdragsgivare att den skyldige förmodligen stod att finna bland Alphacash delägare.

En stark känsla av olust sköljde över Jesper Öhnstedt i samma stund som han klev in genom dörröppningen till Mastercards mötesrum, och möttes av blickarna från över tjugo personer iklädda mörka kostymer och dräkter.

»Nu är det allvar«, tänkte han.

Utänför var det en kall onsdagsförmiddag den 13 mars och vid ett långt ljusst mötesbord på fjärde våningen i en av Sergelsskraporna i Stockholm träffade han och Jonas Petersson storbankernas säkerhetspersonal öga mot öga för första gången.

Enligt inbjudan skulle mötet handla om »restaurantincidenten«.

Mycket mer visste de inte.

Nu ställde representanter för alla de fyra storbankerna samt Strålfors, Visa och Mastercard frågor om Alphacash säkerhetsrutiner.

– Vad vet ni om Strålfors Auriga-server? frågade någon.

– Hur många brandväggar har ni på kontoret?

– Vad vet ni om PCI DSS-autentisering?

Ju längre mötet fortgick, desto mer insåg Jonas och Jesper att många av frågorna handlade om sådant som bara Mattias Eriksson kunde svara på. Men han var i Brasilien, för andra gången på ett halvår. För att fira sin trettioårsdag och för att hämta hem

sin nyblivna flickvän till Sverige.

De fick frågor om en olovlig transaktion gjord på en av innekokarna i Norrköping, restaurang Carl Johan. Ett köp på 50 000 kronor hade gjorts med ett Mastercard Gold kopplat till ett konto i Hongkong. Omedelbart efter godkännandet gjordes ett återköp på samma summa, men istället för att hamna på Mastercard-kortet fördes summan över till ett svenskt Nordeakort.

Jonas och Jesper satt som två stora frågetecken.

– Nä, så fungerar det inte, det ska inte ens gå att göra så, började Jonas.

Sedan kom han på att för den som hade tillgång till ett administratörskonto, skulle det säkert vara teoretiskt möjligt.

– Men det är definitivt inte vanligt, sade han.

När mötet var över tog Jonas och Jesper hissen ner från Mastercards kontor. De bara tittade på

## EN GLOBAL FARROT

I takt med att betalningssystemen digitaliserats har brottsligheten följt efter. Filter listar de senaste årens mest omfattande attacker.

### 1. NETFILL-SKANDALEN, 1998

Kenneth Taves, Kalifornien

Porrföretagaren i Malibu anslöt på eget bevåg 900 000 kortkunder till sina barnförbudna betaltjänster på Internet. Drygt hälften av de drabbade ägde inte ens en dator, men under åren 1997 till 1998 kom Ken Taves över 37,5 miljoner dollar. Han dömdes 2004 till elva års fängelse. En medhjälpare till Taves flydde till Jamaica och har ännu inte dömts för brott.

### 2. ALFABANK/UNIONCARD-HÄRVAN, 1999-2000

Andrej Golov, Ryssland, Magnus Jakobsson, Sverige

Säkerhetschefen och krypteringsexperten på en av Rysslands största banker Alfa Bank, Andrej Golov, utnyttjade sin position till att komma över 300 000 kortnummer med tillhörande pin-koder. Med hjälp av svensken Magnus Jakobsson tillverkades nya plastkort med vars hjälp tiotals miljoner kronor plockades ut i uttagsautomater av lokala kriminella gäng runt om i Europa, innan Magnus Jakobsson greps och härvan nystades upp.

### 3. CARDSYSTEMS, 2005

Hackergrupp, USA

Hackare utnyttjade säkerhetsbrister hos företaget CardSystems, som skötte korttransaktioner åt Mastercard och Visa. Med hjälp av ett virusliknande program som hackarna placerade inne i företagets datasystem kom man över 200 000 kortuppgifter med kortnummer, kortinnehavarens namn och koder. Totalt beräknas 40 miljoner kortnummer ha exponerats innan attacken avslöjades.

### 4. TJX-HACKERS, 2006

Hackergrupp, USA, Ukraina, Kina, Estland och Vitryssland

Elva personer av olika nationaliteter åtalades 2008 för att under ledning av den amerikanske medborgaren och Secret Service-informatören Albert »Segvec« Gonzalez ha kommit

över minst 41 miljoner butikskunders kortnummer värda miljontals dollar på den svarta marknaden. Kortnumren stals med hjälp av ett virusprogram som placerats i stora butikskedjors trådlösa nätverk.

### 5. GUDFADERN, 2007

Maxim »Maksik« Jastremskij, Ukraina

Maxim »Maksik« Jastremskij misstänks för inblandning i de flesta stora attackerna mot amerikanska finansiella institutioner de senaste fem åren. Dömdes i januari 2009 av en turkisk domstol till 30 års fängelse för att ha hackat sig in i tolv banker och sålt stulen kortinformation för totalt elva miljoner dollar. Är en av de huvudmisstänkta i den så kallade TJX-skandalen ovan.

### 6. CARDERSMARKET-KUPPEN, 2006-2007

Max »Iceman« Butler, San Francisco

Under några få dagar i augusti 2006 hackade sig Max Butler in i andra internetbedragares forum för försäljning av stulen kortinformation, för att själv ta kontroll över hela den miljoninbringande marknaden. Ett efter ett släcktes forumen ner och användarna hänvisades istället till Butlers skapelse CardersMarket.com, som kom att bli den största svarta kortmarknaden i världen, tills Secret Service i september 2007 stormade Max Butlers hem.

### 7. THE ROCK PHISH GANG, 2005-

Hackergrupp, okänd hemvist

Toppar amerikanska Secret Service lista över eftersökta internetbrottslingar. Bakom namnet Rock Phish finns troligtvis en grupp hackers som ligger bakom hälften av alla phishingattacker i världen, där till exempel bankkunder med hjälp av falska e-postmeddelanden manövreras till en kopia av sin egen internetbank där all information de knappar in går till bedragarna. Gruppen tros ha tjänat tiotals miljoner dollar på sin verksamhet.



varandra och skakade på sina huvuden. De kände att något stort var under uppsegling som de inte hade kontrollen över.

Först när de kom ut på gatan bröts tystnaden av Jonas Norrköpingdialekt:

– Jag tror att det är någon som har en del att förklara när han kommer hem.

Mattias Eriksson var den som skötte servicen åt kunderna. För sin egen bekvämlighet hade han ett fjärrstyrningssystem som lät honom logga in i kassaterminalerna på distans. Därmed kunde han också vittja dem på information, var han än befann sig. I teorin fanns det inget som hindrade honom från att sedan skicka den vidare till en utomstående person som tillverkade nya plastkort med informationen.

När Mattias Eriksson kom hem från Brasilien försökte Jesper Öhnstedt prata med sin kompanjon om problemet, men fick bara undanligande svar. Det var en märkbart stressad Mattias som Jesper Öhnstedt fick med sig till ett nytt möte uppe på Mastercard en vecka efter det första. Nu räckte den engelske utredaren fram ett fax med en kopia av ett körkort till delägarna för Alphacash.

Cybertrusts säkerhetsexpert berättade att mannen på körkortet var identisk med ägaren till de två bankkort som använts vid den omtalade överföringen på restaurang Carl Johan.

Jesper Öhnstedt granskade bilden, men den sade honom ingenting. Utredaren frågade om han inte kände igen mannens namn. Inte heller det hade Jesper hört talas om. Samma svar gav Mattias Eriksson.

– *It's a very bad man*, sade utredaren allvarligt, och verkade bestört över att två personer som arbetade med kassasystem i Sverige inte var bekanta med namnet.

Mannen på bilden var Magnus Jakobsson.

En kväll några dagar senare ringde telefonen hemma hos Alphacashfinansören Håkan Tegelberg i Kungälv. Han hörde en panikslagen röst i luren:

– Jag är hos dig om en timme. Jag måste sticka. Det var Mattias.

Håkan Tegelberg undrade om det hade hänt Mattias flickvän något. Han visste att de hade kommit

från Brasilien bara ett par dagar tidigare och att hon var i Sverige för första gången. Nu skulle de tillbaka med vändande flyg.

Mattias varken lyssnade eller förklarade:

– Vi kommer nu. Vi måste sticka, sa han.

När Mattias kom innanför dörren till Håkan Tegelbergs villa såg han lika panikslagen ut som han hade låtit i telefonen.

Han berättade en historia som gick ut på att han blivit mordhotad av en restaurangägare i Norrköping. Denne beskyllde Mattias för att ha sålt en kassaterminal som gjorde att polisen kunde uppdaga ett skattebedrägeri. Nu menade Mattias att hans enda utväg var att fly landet.

Håkan försökte lugna ner honom och förklarade att det måste finnas andra sätt.

Under kvällen lade Mattias Eriksson plötsligt upp en tjock bunt med sedlar på vardagsrumsbordet inför Håkan Tegelberg och hans familj. Det var närmare 200 000 kronor. Enligt Håkan Tegelberg hade Eriksson dessutom väskorna fullprop-pade med nyinköpta laptoppar och andra elektronikvaror.

Nästa dag tog Mattias Eriksson och hans flickvän bilen till Oslo och Gardemoens flygplats. Klockan närmade sig fyra på eftermiddagen den 24 mars 2007 när Air France flight AF2375 lyfte för att ta dem till Paris, och därifrån vidare till Brasilien och Natal.

För Norrköpingspolisen kom Jesper Öhnstedts anmälan av Mattias Eriksson som en blix från klar himmel. Utöver spridda, till synes separata fall av kontokortsbedrägerier, fanns ingen samlad anmälan om mer storskalig brottslighet. Namnet Alphacash var okänt. Det fanns ingen utredning, ingen anmälan, ingenting. Polismännen var frustreerade. Bankerna hade gjort som de brukade. De hade skött utredningen själva.

Och nu hade den huvudmisstänkte i vad som kunde vara den hittills största kortsvindeln i Sverige redan dragit till ett land han inte kunde begäras utlämnad ifrån.

Först ytterligare ett par dagar senare, den 29 mars 2007, lämnade SEB som första bank in en polisanmälan. Veckorna därpå följde de andra storbankerna efter.

Det dröjde ytterligare fem veckor innan

uppgifterna om att någonting hade hänt sipprade ut till allmänheten. Då hade mer än tre månader gått sedan den första stora bedrägeriattacken i Tempo-butiken på Djurö. Bankernas utredning hade pågått nästan lika länge.

Den 7 maj avslöjade Dagens industri att Euro-card sänt ut brev till över tusen kunder i Sverige där företaget förklarade att deras kortnummer kunde ha hamnat i orätta händer. Eurocards kort är bland de mest eftertraktade bland kortbedragare eftersom de ofta saknar övre uttagsgräns. Nu skulle tusen kort bytas ut »i förebyggande syfte«.

»Vi har fått signaler. Men jag kan inte gå in i detalj på hur vi snappar upp det här«, sa Sofia Fjellestad, marknadsansvarig på Eurocard till Dagens industri.

Dagen därpå bekräftade SEB att tiotusen av bankens kort skulle bytas ut.

»Detta är större än vi först trodde«, sade bankens informationschef Kerstin Ottosson.

Journalisterna fick bokstavligen dra ut informationen från bankerna och först ett par dagar senare medgav också SEB:s konkurrenter att de var drabbade.

Handelsbanken berättade att 5 268 kunder skulle få nya kort, hos Nordea låg siffran på drygt 20 000. Den största kortutgivaren Swedbank erkände visserligen att man drabbats, men har än i dag inte angett någon siffra, med motiveringen att man aldrig redovisar den typen av uppgifter.

Finansinspektionens enhet för kredit och operativa risker fick beskedet om det stora läckaget av kortinformation via media, och bad om en förklaring. En första kontakt togs med SEB, som – samtidigt som informationschefen sagt till medierna att tiotusen kort bytts ut – meddelade Finansinspektionen att den korrekta siffran var 24 000 kort.

Precis som är fallet med nästan alla större amerikanska uppfinningar finns det en svårkontrollerad anekdot knuten till hur det första kreditkortet kom till. Den inleds med en dyr nota på en exklusiv affärsrestaurang på Manhattan, den 28 februari 1950.

Affärsmannen Frank McNamara hade just avslutat en middag med ett par affärsbekanta och deras fruar när han upptäckte att plånboken inte låg på sin plats i kavajens innerficka. Frank McNamara

## »Eurocards kort är bland de mest eftertraktade bland kortbedragare eftersom de ofta saknar övre uttagsgräns. Nu skulle tusen kort bytas ut i förebyggande syfte.«

ville ändå upprätthålla skenet när notan kom in, och kontaktade hovmästaren. Diskret räckte McNamara honom ett av sina visitkort som han signerade baktill, med en uppmaning att skicka räkningen till hans kontor dagen därpå.

Samma år grundade Frank McNamara företaget Diners Club. Innan året var slut hade han gett ut 200 kort som accepterades på 27 exklusiva restauranger och två lika exklusiva hotell i området runt Wall Street.

Det var naturligtvis ingen tillfällighet att just Frank McNamara, känd och betrodd gäst, slapp diska sig från notan den där februarikvällen 1950. Liksom alla tidigare kända betalningsmedel är kreditkortet framför allt en fråga om förtroende.

Redan före vår tideräkning präglades mynt med kejsarens bild eller den härskande maktens symboler som garant för myntets värde. De första svenska sedlarna bar namnunderskrifter från alla riksbankens ledamöter för att inge förtroende och en

# FRÅN SNÄCKA TILL CHIP

Smidighet och förtroende har alltid varit ledorden för utvecklingen av människans betalmedel. Det ska vara enkelt att handla, och det ska gå att lita på att det jag får i handen när jag säljer en vara betingar samma värde dagen därpå.



## FÖRE 1000 F.KR.

Kaurisnäckan var den viktigaste valutan i forntida Kina, Indien, Sydostasien och Afrika. Liksom andra tidiga betalningsmedel hade den flera användningsområden, bland annat som prydnadsföremål. Chokladbönor och metallbitar var andra tidiga betalningsmedel.



## CA 650 F.KR.

Det första myntet tillverkades i kungariket Lydien i främre Asien av elektrum, en naturlig legering av guld och silver. Dess värde var identiskt med metallvärdet. Kungamakternas symbol, lejonet, garanterade dess äkthet.



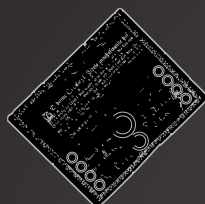
## 200-TALET F.KR.

Den romerska denaren kom med det romerska rikets etablering som världsmakt att gälla som huvudvaluta i all internationell handel. På så sätt var denaren en föregångare till dagens dollar och euro.



## 1518

I tyska Joachimsthal präglades den nya tidens första internationellt gångbara valuta, talern. Alla härskare i norra Europa präglade mynt till samma halt och vikt vilket gjorde talern (på svenska daler) till den stora gränsöverskridande valutan fram till 1700-talets mitt.



## 1661

Sverige var först i världen med att ge ut banksedlar av papper. De skulle bara utlämnas åt dem som satte in motsvarande mängd mynt, men det efterlevdes inte och riksbanken gick i konkurs efter sju år. Grundaren Johan Palmstruch dömdes till döden (men benådades).



## 1795

I efterdyningarna av den franska revolutionen infördes den första valutan med decimalsystemet som grund (1 franc = 100 centimes), vilket förenklade kontanthandlingen avsevärt.



## 1890-TALET

Amerikanska varuhus införde charge coins – numererade metallbrickor som gav kunden rätt att handla på kredit. Uppgifterna kontrollerades mot en förteckning som fanns i kassan. Nordiska Kompaniet införde ett liknande system under 1930-talet.



## 1951

Med visitkortet som förebild tillverkade Frank MacNamara det första moderna kreditkortet, Diners Club. Materialet var papp och ursprungligen accepterades kortet bara på lyxrestauranger runt Wall Street.



## 1958

BankAmericard, föregångaren till Visa, lanserades i Kalifornien. Samma år sjöattes American Express, som redan första dagen fick in 275 000 kortansökningar från allmänheten. 1966 lanserades Mastercard.



## BÖRJAN AV 1960-TALET

Londons tunnelbana införde det första betalkortet med magnetremsa. Tio år senare blev magnetremsan standard även för kontokort.



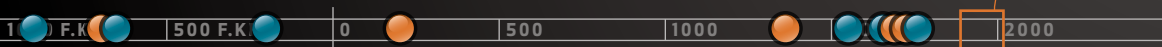
## 1967

I Londonförorten Enfield öppnade Barclays den 27 juni 1967 världens första uttagsautomat, med komplicerad hållkortsteknik. Redan en vecka senare fanns den första svenska uttagsautomaten på plats vid Uppsala Sparbanks kontor vid Stora Torget i Uppsala.



## 1978

Den franske uppfinnaren Roland Moreno uppfann chiptekniken. Den introducerades snabbt på telefonkort, men det dröjde en bit in på 80-talet innan franska banker blev först i världen med chipförsedda betalkort. Svenska bankkort med chip debuterade 2004.



## FÖRFÄLSKARE OCH BEDRAGARE

### FÖRE 650 F.KR.

Genom att manipulera vågarna lurade korrupta köpmän till sig fler silver- och guldstycken än de egentligen skulle ha för sina varor. På motsvarande vis lät oärliga köpare gravera in förtroendegivande stämplor på metallstyckena, som inte stämde överens med deras faktiska halt och vikt

### 220 E.KR.

Under denarens höjdpunkt bestod den av 98 procent silver. Återkommande ekonomiska kriser i det romerska imperiet fick kejsaren att späda ut denaren så att den på ett par årtionden förvandlades till ett kopparmynt. För att dölja försämringen doppades mynten i silverbad men det förhindrade inte att den upphörde att fungera som internationellt handelsmynt.

### 1670

För att komma åt värdefull metall filade eller klippte bedragare bort delar av mynt utan att det märktes. Som motåtgärd infördes 1670 den första randskriften på ett svenskt mynt, »manibvs ne laedar avaris« (må jag icke skadas av giriga händer). I dag underlättar ornamenten på myntens rand för synskadade och låter myntautomater skilja mellan olika valörer.

### 1755

Trots tidigt användande av vattenmärke, silvertråd och att alla sedlar bar en mening om att straffet för förfälskning var hängning, skenade förfälskningen i takt med tryckteknikens spridning. 1755 grundade därför Sveriges Riksbank Tumba Bruk för att tillverka unikt papper för sedelutgivningen.

### 1988

Checkbedrägerierna nådde sin höjdpunkt i Sverige, med 17 000 fall. Några år senare var checken på utdöende som betalningsmedel.

### 1999

Konsumenttidningen Råd & rön rapporterade för första gången om det nya fenomenet skimming.

### 2002

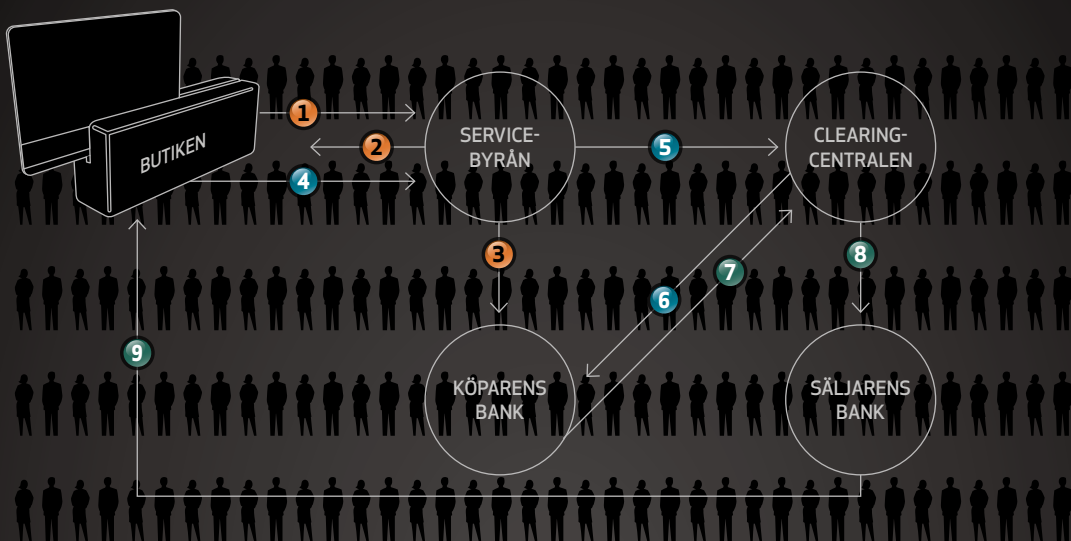
Fenomenet »phishing« – att bedragare lurar till sig kontoinformation via falska Internetsidor eller e-post – nådde Sverige. Mastercards kunder fick ett e-postmeddelande från en Mastercardadress och uppmanades att klicka på en länk som tog dem till en exakt kopia av Mastercards hemsida. När kunderna skrev in sina kontouppgifter och lösenord skickades informationen till bedragarna.

### 2005

Den första »pharming«-attacken i USA. Pharming innebär att datahackers bryter sig igenom exempelvis en banks säkerhetssystem, och gör så att kunder som loggat in sig på bankens »säkra« hemsida omdirigeras till en falsk sida där kunden sedan slår in sina kontouppgifter.

# EN TRANSAKTION – TUSEN ÖGON

Det som tidigare var en transaktion mellan köpare och säljare är i dag en komplicerad, landsöverskridande process i många steg och med en mängd institutioner inblandade.



## FAS 1 BETALNINGEN

### BUTIKEN

Kortet dras i butikens kortterminal. Köparen bekräftar att hon/han är innehavare av kortet genom namnunderskrift och legitimation eller pin-kod. Butiken kontaktar Servicebyrån (1) för ett snabbgodkännande av köpet.

### SERVICEBYRÅN

Är kortet spärrat? Finns den efterfrågade summan på det till kortet kopplade kontot? Servicebyrån skickar ett sekundsnabbt godkännande (2) eller felmeddelande till betalterminalen ihop med ett unikt kontrollnummer. Samtidigt skickas ett meddelande (3) till köparens bank, som reserverar det aktuella beloppet.

## FAS 2 CLEARINGEN

### BUTIKEN

Butikens kassa stämplas ut vid dagens slut. Mer detaljerad kortinformation skickas till servicebyrån (4).

### SERVICEBYRÅN

Servicebyrån sammanställer betalningsuppdragen från en mängd butiker och sänder dem vidare till kortutgivaren för clearing (5).

### CLEARINGCENTRALEN

Av den kortutgivande banken i Sverige, eller av kortorganisationerna Visa eller Mastercard i London respektive Bryssel, sammanställs köparens betalningsförpliktelser till en utbetalningsorder som skickas till köparens bank (6).

## FAS 3 INLÖSEN

### KÖPARENS BANK

Den reserverade summan dras från köparens konto, och skickas till clearingcentralen (7).

### CLEARINGCENTRALEN

Clearingcentralen överför pengarna till butikens bank (8).

### SÄLJARENS BANK

Två till sju dagar efter att kunden har dragit sitt kort finns pengarna tillgängliga för företaget som äger butiken (9).

15,1

antal miljoner betalkort som fanns i Sverige 2007, 6,1 miljoner av dem var kreditkort.

KÄLLA: BANKFÖRENINGEN

1,2

antal miljarder transaktioner med bank- och kreditkort i Sverige 2007.

KÄLLA: BANKFÖRENINGEN

233

antal miljarder kontantlösa transaktioner i världen 2007.

KÄLLA: BANKFÖRENINGEN

garanti att den sköra papperslappen när som helst kunde bytas mot klingande silver.

Kortsystemet bygger på att säljaren av en vara kan lita på att den virtuella summan i kassaterminalen verkligen kan växlas in i reella pengar. Samtidigt måste kunderna kunna lita på att deras pengar är i trygga händer hos kortföretagen.

Magnetremsan är en enkel metod för att lagra information som dessutom är relativt felfri. Men dess enkelhet gör den också lätt att kopiera. Säkerhetsmässigt har magnetremsan beskrivits som det moderna kortsystemets akilleshäla.

I dag kan vem som helst köpa en kombinerad kortläsare och skrivare för tillverkning av egna plastkort för ett par hundralappar via butiker på internet. Samma teknik som används av företag och bostadsrättsföreningar för att tillverka passerkort, kan användas till att skapa egenhändigt tillverkade betalkort.

Kort med magnetremsa är en usel produkt. Det är inte svårare att ändra den lagrade informationen än det är att spela in musik på ett kassettband, sade chefen för rikskriminalens finanspolis Marcus Qvennerstedt redan 2001.

Ätta år senare har alla kort som ges ut i Sverige kompletterats med säkerhetsdetaljer som det glittriga hologrammet på Visakorten, och den så kallade CVV-koden som ökar säkerheten vid betalningar på internet. På kortens framsida finns numera ofta det säkrare chipet, en elektronisk krets som kan krypteras hårdare och är betydligt svårare att knäcka för en bedragare.

Övergången från magnetremsa till chip är ett ofantligt projekt: det finns 2 800 uttagsautomater i Sverige, och mer än 187 000 kassaterminaler ute i butiker och restauranger. Handlarnas samarbetsorganisation Svensk handel uppskattar att den mer eller mindre framtvingade nyordningen kostar butikerna en miljard kronor bara i år. Sedan den första mars i år ersätter inte bankerna de handlare som utsatts för kontokortsbedrägerier vid köp där enbart magnetremsan har använts.

Samtidigt är inget system starkare än sin svagaste länk. Så länge korten har kvar magnetremsan kan de kopieras och användas nästan var som helst utanför Sverige. Flera av våra vanligaste semesterorter har

ännu inte påbörjat övergången till chipteknik, och den ledande ekonomiska världsmakten USA har hittills inte visat något intresse för att gå ifrån magnetremsan – eller ens infört pinkoder för bankkort.

Händelser som Alphacashhärvan och Andrej Golovs kupp mot Alfa Bank visar också att moderna bedrägerier lika väl kan ske innanför bankernas noggrant uppbyggda skyddsmurar.

Kritiker menar att bankerna avslöjar så lite som möjligt när de utsätts för attacker, för att inte rubba folks förtroende och riskera en fördröjning av det kontantlösa samhället och investeringarna i nya chipläsare. Svensk handels säkerhetschef Dick Malmund efterfrågar en betydligt större öppenhet från bankerna.

– De vill ju inte exponera svagheter i systemen därför att det blir dyrare för dem, men även då tappar folk förtroendet. Man måste vara ärlig. Jag tror att det handlar om att man har större problem än vad man vill torgföra, framför allt tror jag att man inte känner att man sitter på trumf.

ett e-postmeddelande som gick ut till de övriga delägarna några dagar efter flykten, medgav Mattias Eriksson att han hade haft en långvarig kontakt med den dömda kontokortsbedragaren Magnus Jakobsson, men att de träffats på internet av en tillfällighet när han sökte affärskontakter i Asien. »Under denna tid så jobbade han sig in i vårt system«, skrev Eriksson. »Resultatet av detta blev att han kom åt en massa kortnummer från vårt system.«

Men mest verkade han tycka synd om sig själv: »Vad kan jag säga annat än att jag inte sitter på någon drömsits just nu, i ett skitland utan en spänn på fickan. Jag hoppas att jag någon gång kan ordna upp saker och ting. Detta är inget som jag har gjort med uppsåt. Hoppas att ni förstår och att allt löser sig.«

Det gjorde det inte.

När kontoutdragen från företagskortet damp ned i brevlådan uppe på Alphacash kontor, upptäckte Jonas Pettersson och Jesper Öhnstedt att pengarna som finansierat Mattias Erikssons tomtköp i Natal till större delen kom från deras företagskonto. Dessutom hade landsflyktingen tömt företagskortet och maxat krediten innan han satte sig på flygplanet till Brasilien.

Snart kontaktades Jonas Pettersson och Jesper Öhnstedt dessutom av skattemyndigheten som krävde dem på hundratusentals kronor i obetalda skatter, pengar de trodde att Mattias Eriksson låtit bli att betala under två års tid.

De båda vännerna startade ett nytt kassaterminalbolag, men utan integrerade kortläsare. I ett brev till en av storbankernas säkerhetsansvariga undrade de om det fanns någon framtid för dem inom branschen.

Svaret de fick: »Det kan konstateras att Alpha Cash säkerhetsarbete och tänk kring hur man hanterar känslig kortinformation har varit helt obefintlig och dessutom haft inslag av olaglig verksamhet. Det strider mot minsta tänkbara sunda förnuft och mot samtliga punkter i PCI Data Security Standard som reglerar hur kortinformation får hanteras vilket fått mycket stora konsekvenser för kassakunder, banker, kortinnehavare och flera andra parter.«

Jonas Pettersson och Jesper Öhnstedt tolkade det som ett nej.

**S**amtidigt fortsatte bedrägerierna med kortuppgifter som läckt från Alphacash terminaler. Attackerna skedde från alla världens hörn, och utan tydliga kopplingar till Sverige. Det är troligt att en del av kortinformationen sålts för en dollar styck på något av de skyddade forum för kriminella hackers, skimmare och identitetstjuvar som finns på internet.

Med Mattias Eriksson utflugen och Magnus Jakobsson boende i Thailand gick polisens arbete trögt.

På nystartade hemsidan [www.flytillbrasilien.se](http://www.flytillbrasilien.se) kunde utredarna följa Mattias Erikssons liv på andra sidan Atlanten. »Våga släpp taget och fly till Brasilien«, skrev Eriksson. »Var med om att bygga din dröm utanför Sverige. Investera i Natal, Brasilien. Billigare än så kan det inte bli. Varför lägga alla pengar på skatt och moms i Sverige när man kan åka till Brasilien och starta upp en verksamhet för en bråkdel av pengarna vad det skulle kosta i Sverige?«

Eriksson tipsade den hugade om att Norge som icke EU-land inte delade utreseinformation med Sverige, och att Gardemoen därför var den bästa platsen att rymma ifrån. Han uppgav också matnyttig information som det lokala priset på en flaska Smirnoff eller en påse fryst pommes frites,

samt att stället var i stort behov av en pizzabagare. På hemsidan förbannade han de medier som skrev om Alphacash-härvan, och utmålade sig själv som utsatt för en komplott.

Trots bankernas stora kortbytesprogram fanns fortfarande fungerande kort på vift. Under hösten 2007 drabbades Strålfors av ett allvarligt dataintrång, som innebar att falska kortköp för omkring en miljon kronor kunde göras direkt i Strålfors system. När kortköpet var godkänt gjordes omedelbart ett returköp där pengarna fördes över till andra bankkonton. Kortinformationen som användes kom återigen från Alphacash, och när de IP-adresser som användes vid intrånget bland annat spårades till Brasilien och Thailand ansåg sig utredarna kunna knyta både Mattias Eriksson och Magnus Jakobsson till brottet.

I slutet av december begärde åklagaren Karl-Erik Esbo i Göteborg dem häktade, och sände ut en internationell efterlysning.

Några dagar senare skickade Magnus Jakobsson ett fax till tingsrätten där han förklarade sig oskyldig till alla anklagelser, och begärde att få förre justitieministern Tomas Bodström som försvarsadvokat.

Jakobsson hade skapat sig ett nytt liv i Thailand efter tiden i fängelset, bildat familj och fått ett bra jobb i Hong Kong, som han förlorade som en följd av anklagelserna mot honom.

**D**en 10 januari 2008 klev Magnus Jakobsson ensam in på polishuset i Göteborg och anmälde sig i receptionen. Väl hos polisen sade han ingenting på sju veckor.

– Jag försökte prata med honom men han var inte så värst pratsam, säger Bengt-Åke Nilsson som höll i utredningen vid länskriminalpolisens utredningsrotel.

Magnus Jakobsson delade bankernas uppfattning att systemet var osäkert, men nekade till att ha haft något alls med bedrägerierna att göra. I stället menade han att det var hans gamla dom från 2001 som gjorde att han misstänktes för inblandning i läckaget kring Alphacash terminaler.

– Ett tema när vi höll förhör med honom var att han hade inblick i vad det här handlade om, men han menade att den insynen hade han fått av andra skäl än för att begå brott, säger Karl-Erik Esbo.

Ungefär samtidigt som Magnus Jakobsson

började prata, tystnade bankerna. Polis och åklagare som beskriver att de tidigare haft ett bra samarbete med bankernas säkerhetsavdelningar, fick inte längre svar på sina frågor.

Vilka konton var inblandade? Hur stora var summorna? IP-nummer, tider, datum?

En allt mer stressad Karl-Erik Esbo skrev ett brev till bankerna, med en kopia till Magnus Jakobssons advokat Thomas Bodström, där han förklarade att det nu fanns en man frihetsberövad, och att det därför var extra viktigt att bankerna svarade snabbt på polisens frågor.

– Jakobsson ställde krav på att vi skulle gå till-

baka till bankerna och få nya uppgifter, och jag tyckte inte att jag fick den information som jag önskade för att känna mig trygg att fortsätta ha honom frihetsberövad, säger åklagaren.

Han fick aldrig något svar på brevet.

– När jag inte fick de svar jag behövde så hävde jag häktningen. Och det stannade väl där helt enkelt, säger Karl-Erik Esbo.

I slutet av november 2008 lade han ned förundersökningen. I en bilaga till beslutet skriver han att de brott som utretts i ett och ett halvt års tid »verkligen verkar ha begåtts«, men att utredningen inte kunnat visa vem eller vilka som begått dem.

Hos polisen i Norrköping och Stockholm mottogs nedläggningen med bestörtning.

– Det var inte oväntat, men tråkigt, säger Kaj Hahne vid Stockholmspolisens bedrägerirotel. Det är komplicerade utredningar och när en av de huvudmisstänkta inte finns kvar i landet blir det ännu svårare.

Han är starkt kritisk till hur bankerna och framför allt deras utredare skötte saken från första början:

– Här går bankerna upp med en privat utredare och sätter hårt mot hårt mot den som är huvudmisstänkt, utan att ha en sheriff med sig. Sedan går

man därifrån. Vi hade gått tillväga på ett helt annat sätt. Med den utredning som fanns till grund hade vi kunnat gripa, eller i vart fall gått till åklagare och ordnat med ett reseförbud.

Den enda som åtalades för Alphacashsvindeln var den mångfacetterade fiffelaren »Jean Naaoum«. I juni 2008 dömdes han till ett år och nio månaders fängelse, samt utvisning.

Lars Vikström, nu pensionerad informationssäkerhetschef för Handelsbanken, fick en form av samordnande roll för bankerna under utredningen. Han säger att man aldrig fick något brev från åklagaren.

– Jag tyckte att vi hade ett jättebra samarbete

## »Jag tyckte att vi hade ett jättebra samarbete med polisen och jag tyckte att jag gav dem all den information som vi hade. Men tyvärr räckte det inte hela vägen.«

med polisen och jag tyckte att jag gav dem all den information som vi hade. Men tyvärr räckte det inte hela vägen. Jag beklagar det lika mycket som åklagaren.

Samma inställning redovisar alla de fyra storbankerna samstämmigt. De understryker att alla kunder gjorts ekonomiskt skadelösa och att de egna åtgärderna förhindrat verkligt stor skada som en följd av läckaget.

Bankerna är också överens så till vida att de inte vill ge en totalsumma på antalet berörda kort i Alphacash-härvan.

Enligt en av Sveriges främsta experter på IT-säkerhet, Joakim von Braun på företaget High Performance Solutions, har bankerna bytt ut »betydligt fler än 80 000 kort«.

Uppskattningen stämmer väl överens med den

uppgift om 24 000 utbytta kort som SEB gav Finansinspektionen i början av maj 2007, före härvans kulmen och intrånget i Strålfors.

SEB står som utgivare för drygt en tredjedel av landets nio miljoner kort, och det har inte framkommit några uppgifter om att de skulle ha varit hårdare drabbade än några andra banker. Tvärtom är det rimligt att anta att alla bankkunder utsatts för en likvärdig risk. Bankerna skulle med samma resonemang ha förlorat betydligt mer än tio miljoner kronor.

Det gör kortsvindeln till den största hittills i svensk historia.

Det finns ett billigt rum att hyra, bara fem minuter från stranden i turistorten Porta Negra söder om Natal. För 1 200 kronor blir det ditt för en vecka. Då ingår trådlös uppkoppling mot internet, vatten, el och gas.

Att döma av bilden som ligger upplagd på annonsidan Blocket tar en bred säng med aluminiumben upp större delen av det spartanskt inredda rummet.

Det är ett rum i en lägenhet i ett av Porta Negras sämre områden som Mattias Eriksson hyr ut åt svenska turister. Lägenheten har inte mycket gemensamt med de drömmar han hade om ett bekvämt lyxliv i en arkitektritad villa.

– Nu sitter jag här nere, jag har fått skiten för alltihopa och bor i Porta Negras slumområde, stadsdelen som hotellen varnar turisterna för att gå till efter att det har blivit mörkt, den billigaste jävla lägenheten man kan leta reda på, säger Mattias Eriksson när jag når honom på hans mobiltelefon.

Solen sken inte ens första dagen de kom till det nya landet. Flygplatsen i Rio de Janeiro var insvept i en tät dimma och de missade anslutningsflyget som skulle ta dem vidare till Natal.

– Det är ingen jävla dans på rosor här nere. Jobb är omöjligt att få. Det är det liv man har, men jag känner: att åka tillbaka till Sverige, vad har jag där?

Han vidhåller sin förklaring till varför han flydde: han var rädd, inte för polisen eller bankernas utredare, utan för en restaurangägare i Norrköping.

Enligt polisen levde Mattias Eriksson ett utsvävande liv med mycket festande de första veckorna i Brasilien. Mattias Eriksson själv säger att han hade med sig två packade resväskor och 30 000 kronor i kontanter. Oavsett vems bild som stämmer är det uppenbart att pengarna nu är slut.

En gammal barndomsvän skickade ner några tusen med Western Union. Föräldrarna hemma i Krokek har skickat en del. Han säger att han har lyckats få ihop några tusenlappar här och där genom att tillverka hemsidor åt svenska företag, men att det inte rör sig om några större summor.

Tomten med sjuttio meter ned till den brusande Atlanten tvingades han sälja »för att lösa en del skulder« och »för att köpa möbler till lägenheten«.

– Den var svårsåld som fan. Jag sålde den till långt under värdet, säger Mattias.

Livet i Brasilien som skulle ha varit enkelt att leva har blivit till en ständig jakt efter pengar. Alphacash gamla hemsida på Internet har han gjort om till en annonsplats för spelsajter på Internet. Enligt Mattias ger det honom hundra dollar med några månaders mellanrum.

Han har tagit SMS-lån i Sverige på 20 000 kronor som han inte har för avsikt att betala tillbaka och agerar målvakt i ett säkerhetsbolag med kopplingar till den organiserade brottsligheten.

– Det är inga roliga grabbar som äger det där, så jag vill inte bråka med dem. Jag vet inte vad de gör med skiten, men jag fick betalt för det och behövde pengar för att köpa mat och betala min hyra. Jag skiter faktiskt i vad som händer med det bolaget om jag ska vara riktigt ärligt, men jag tvekar inte att göra det igen så länge det handlar om att överleva.

Trots det låter han inte alltför ångerfull:

– Jag ångrar bara en sak, och det är att jag inte gjorde det, för då hade jag i alla fall suttit här med cash.

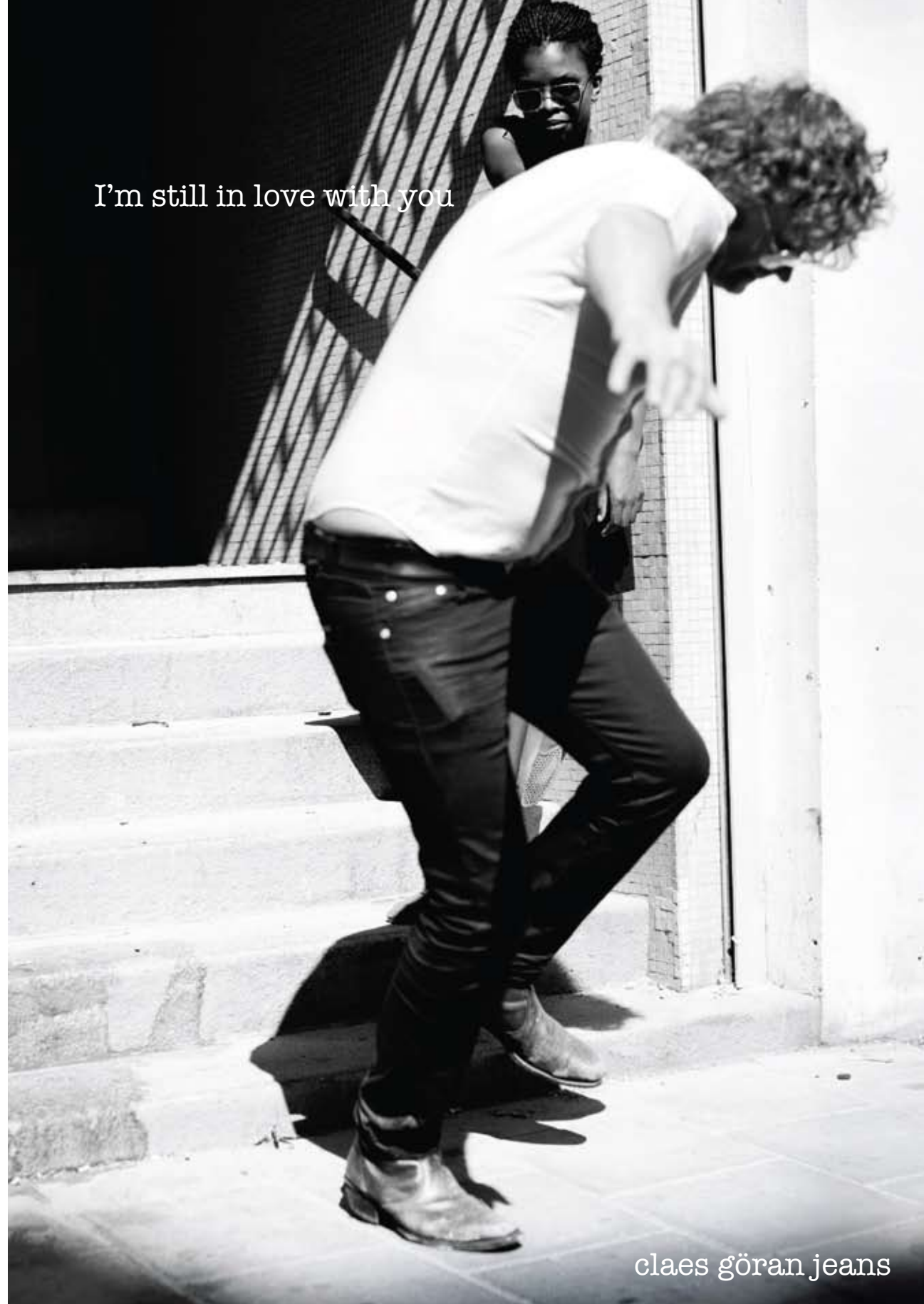
*Fotnot: Magnus Jakobsson har trots upprepade kontakter avböjt sin medverkan.*

*Daniel Olsson är frilansande kriminalreporter och medlem av redaktionen för Grävande journalisters tidning Scoop.*

*Rickard Frank utgör den ena halvan av den prisbelönta designduon NordströmFrank, som bland annat har redesignat Sydsvenskan och Dagens Industri.*

**ONSDAG 1 APRIL** Den nya säkerhetsstandarden PA DSS – som ska förhindra att kortinformation hamnar i orätta händer – börjar gälla för svenska kassaterminaler. Butiker som inte följer den riskerar att stängas av från marknaden.

I'm still in love with you



Growyn är en ny svensk sökmotor som ger bort hela sin vinst till miljön.

[www.growyn.com](http://www.growyn.com)

growyn