ISC 2015 中国互联网安全大会

360互联网安全中心

ISC 2015

数据驱动安全

2015 中国互联网安全大会 China Internet Security Conference

电子取证论坛

盗卡器取证—小心，您的银行卡被盗刷了

个人简介

- 中国电子学会计算机取证专家委员会委员
- 全国电子物证分技术委员会专家工作组成员
- 上海市司法鉴定协会电子数据取证专业委员会委员
- 公安部/司法部 能力验证专家
- 上海辰星电子数据司法鉴定中心 技术主管
- 中国政法大学电子证据研究中心特聘研究员
- 第一届“宋慈”/第二届“鼎永杯”优秀司法鉴定文书获奖者
- 多个公共安全行业标准和司法鉴定技术规范起草者

银行卡的产生和发展

产生和发展

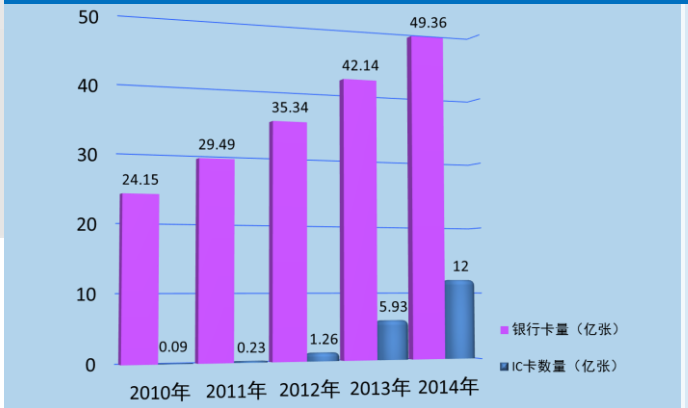
1985' 第一张银行卡--“中银卡”（准贷记卡）发行。

1987' 首台ATM机在广东珠海出现。

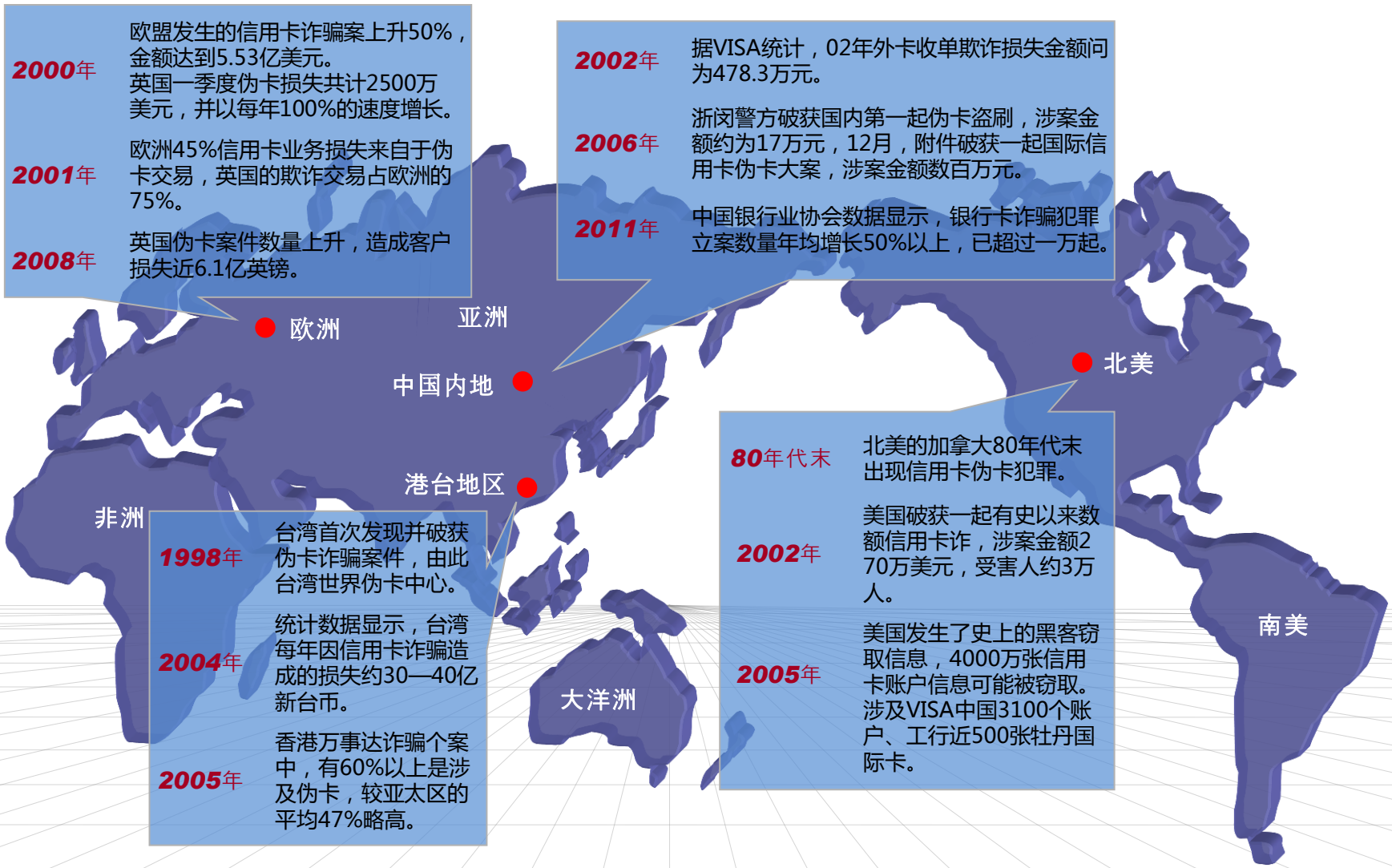
1993' 打通银行卡”的全国“金卡工程”开始启动。

2002' 中国银联在上海成立，宣告中国银行卡体制创新进入新的阶段。

2015' 发卡量增长到7.2亿张；信用卡交易额达到了15.2万亿元；发卡银行从原来的五家增长到近百家。



全世界的伪卡犯罪史



2000年 欧盟发生的信用卡诈骗案上升50%，金额达到5.53亿美元。英国一季度伪卡损失共计2500万美元，并以每年100%的速度增长。

2001年 欧洲45%信用卡业务损失来自于伪卡交易，英国的欺诈交易占欧洲的75%。

2008年 英国伪卡案件数量上升，造成客户损失近6.1亿英镑。

2002年 据VISA统计，02年外卡收单欺诈损失金额问为478.3万元。

2006年 浙闵警方破获国内第一起伪卡盗刷，涉案金额约为17万元，12月，附件破获一起国际信用卡伪卡大案，涉案金额数百万元。

2011年 中国银行业协会数据显示，银行卡诈骗犯罪立案数量年均增长50%以上，已超过一万起。

1998年 台湾首次发现并破获伪卡诈骗案件，由此台湾世界伪卡中心。

2004年 统计数据显示，台湾每年因信用卡诈骗造成的损失约30—40亿新台币。

2005年 香港万事达诈骗个案中，有60%以上是涉及伪卡，较亚太区的平均47%略高。

80年代末 北美的加拿大80年代末出现信用卡伪卡犯罪。

2002年 美国破获一起有史以来数额信用卡诈，涉案金额270万美元，受害人约3万人。

2005年 美国发生了史上的黑客窃取信息，4000万张信用卡账户信息可能被窃取。涉及VISA中国3100个账户、工行近500张牡丹国际卡。

磁条卡介绍

磁条

银行卡磁条的特性、编码技术及编码字符集应符合GB / T15120.2 中的有关要求。所有银行磁条卡必须使用第 2 磁道。第3 磁道是否使用由各发卡机构自行规定。第1 磁道暂不使用，第2 磁道作为交换磁道，各发卡机构在进行识别和信息交换时以第2 磁道为准。

1 第1磁道的信息格式：磁道1为只读磁道，数据编码可记录数字（0 - 9）、字母（A - Z）和其他一些符号（如括号、分隔符等），最大可记录 79 个数字或字母。

2 第2磁道的信息格式：磁道2为只读磁道，所记录的字符只能是数字（0 - 9）和“=”，最大可记录40 个字符。包括：主账号、字段分隔符、失效日期、服务代码、附加数据、结束标志、纵向冗余校验位。

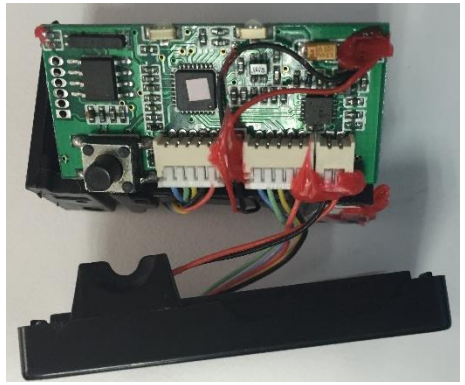
3 第3磁道的信息格式：磁道3为读写磁道，所记录的字符只能是数字（0 - 9），最大可记录107 个字符。

常见的盗卡类型及作案工具

ATM测录

POS机测录

POS机操作员测录



网上公然兜售“克隆银行卡”设备

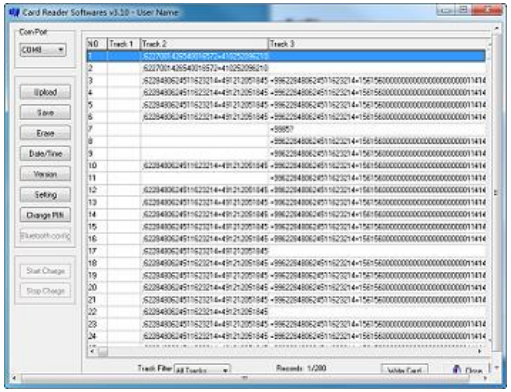
测录器的取证—涉案数据提取

直接读取

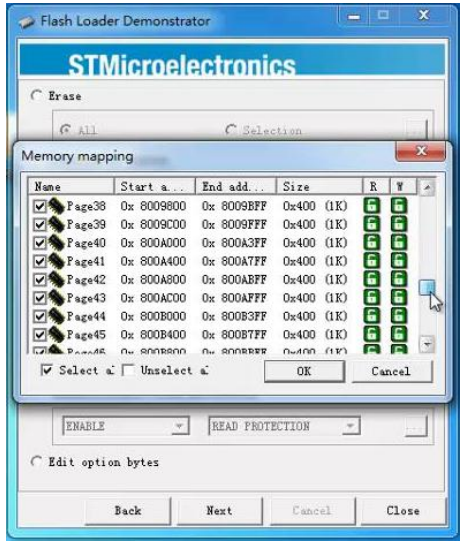
```
   ~H□   9/02/23 22:15:26%996222
02100102182     =1561560000000000
0000030959992160000491200000000
000000000000=000000000000=000000
00?;6222021001021822413=49121200
959991557?+Blank? □□□□□□□□□□□□□□

□□□□□□□□□□□□□□□□? K□   □   □   □
   □   □   ~H□   9/02/23 22:15:3
0%9962220210010218      =15615600
0000000000003095999216000049120
00000000000000000000=00000000000
0=00000000?;Error?+Blank? 22413=
491212009599991557?+Blank? □□□□□□
```

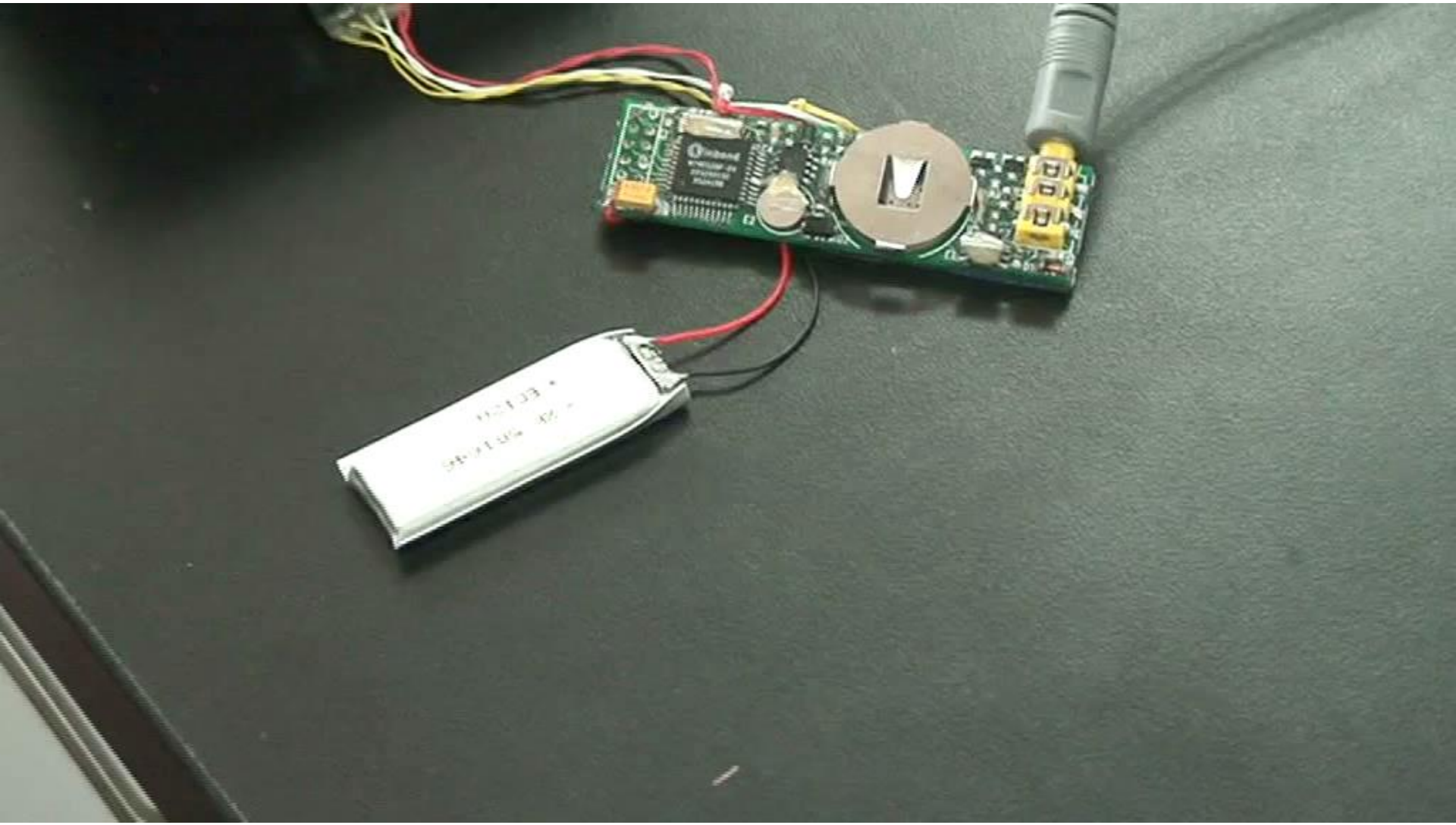
专用程序读取



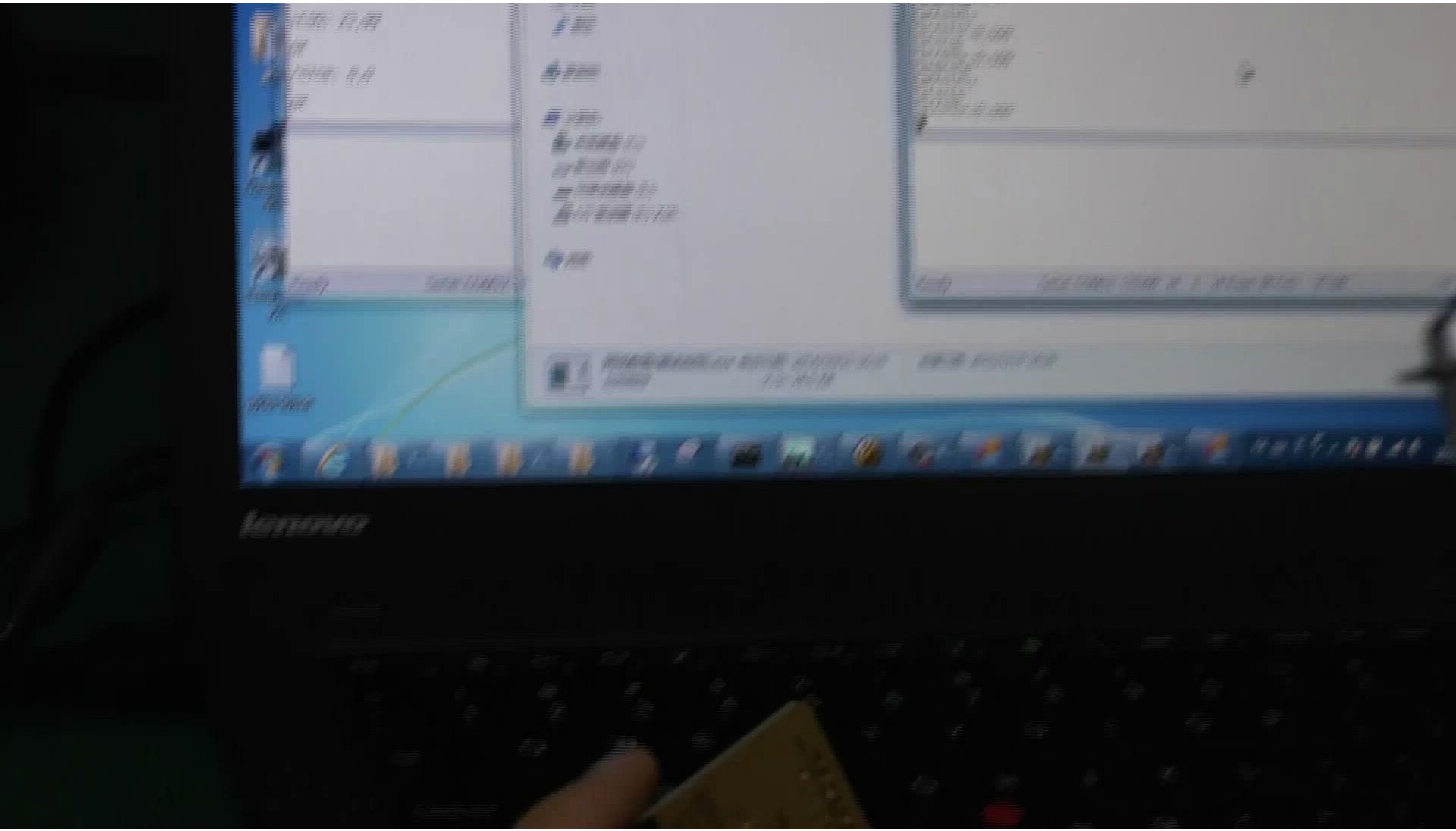
Chip-off读取



ATM测录器的取证—功能检验



POS测录器的取证—功能检验



伪卡犯罪的解决之道

发卡端落实银行卡账户实名制，控制信用卡发卡风险。

受理市场端,建立健全特约商户的监控制度和档案管理制度，加强对ATM的现场监控和巡查。

银行卡交易环节,完善对交易信息的动态监测和可疑交易的监控。

伪卡犯罪的解决之道

金融IC卡

真正杜绝克隆卡、伪卡盗刷仍需更新现有的技术。 利用金融IC卡，能够有效解决目前使用磁条卡时存在的盗卡等安全问题。金融IC卡的交易安全机制，使复制与伪造更加困难，持卡人的资金安全保障大大提高，从而有效防范伪卡盗刷难题。

金融IC卡未迅速升级的原因

1

我国信用卡升级工程最大的障碍就是过于庞大的发卡量。2005年3月《中国金融集成电路(IC)卡规范》标准颁布，却一直未能大范围推广实施，当时的银行卡保有量是9.2亿张，而现在的磁条卡已达37.4亿。

数量大

2

智能IC卡升级工程不仅耗资巨大，而且需要极大的时间成本。由于目前国内银行卡规模庞大，业内专家估计，这一迁移过程预计会耗时10年。

时间长

3

银行磁条卡系统升级成为IC智能卡系统，关系到银行卡、ATM、POS机等终端的改造升级、银行后台计算机系统的升级、银行卡系统工作人员培训等方面的费用，综合计算总耗费将高达1000亿元。

费用高

4

将现有的磁条信用卡全部换成芯片卡会大大提高银行的成本。现在使用的磁条卡每张卡的成本不过是1元多，而如果换成芯片卡，成本将上升到近40元。

成本高

如何防范“伪卡盗刷”

01 申请交易短信提醒

多数遭遇伪卡盗刷的用户都是通过交易短信提醒，发现自己的信用卡被盗刷；而小部分未申请交易短信服务的用户则延误了挂失、报案最佳时机。因此持卡人有必要了解银行提供的短信提醒服务。

02 注意防范盗卡器和保护密码

使用ATM机时一定要细心观察，发现可疑设备时不能贸然使用。输密码时要用另一只手或身体挡住操作手势，如果发觉密码被偷窥，要立即修改密码或联系银行办理密码挂失。

03 刷卡消费全程监督

刷卡消费时收营员有可能备份用户的信用卡资料，须格外谨慎，尤其是酒店消费，持卡人应尽量全称参与刷卡过程，而不应为图方便将信用卡交给服务员代您进行交易。

04 保管好交易凭条

很多储户在办理完业务后，将凭条随意丢弃，这样可能就会泄露储户信息，包括账号、卡号等，因此一定要把交易凭条彻底粉碎或收好。

05 及时挂失和报警

及时联系银行客户服务中心，对卡片进行控管，并办理冻结、挂失或者换卡业务，并且收集有关持卡人不在刷卡现场的证据，例如可以立即持真卡到就近银行反映或向110报案。

电子数据取证与鉴定

谢谢观看