

# 到赌场抵押房产，可以翻倍套现资金？

## 退休男子“闭眼”投资，结果被骗500余万元

本报记者 陈贞妃 实习生 蓝昕宇 通讯员 高佳梨

“2000万元的房子，放到澳门赌场去可以置换4000万元的资金！”在朋友一通劝说下，60多岁的老金（化名）“一掷千金”，将自己的14套房产全部“抵押套现”。结果现实给了他肉痛的一击——他最终被骗走500余万元。

### 资产高额套现的商机

老金是绍兴人，早年经商，经济条件优越，置办下了许多房产。退休后，他依然喜欢投资一些高回报的理财项目。2017年，偶然的一次机会，他在一家古董店认识了40余岁的樊某。两人一见如故，相谈甚欢。

2019年11月的一天，樊某约见老金，告诉他自己的生意有一笔稳赚不赔的买卖，想找他合作。

“我在澳门赌场混迹多年，认识一些内部的人，最近发现了一个资产高额套现的商机。”樊某知道，老金一直等着名下的一些房产增值后套现。他告诉老金，在赌场中，如果赌徒有一些房、车等资产，可以抵押给赌场老板换取高于市值几倍的筹码。

而他有内部渠道，可以跟对方合作，把原本只能在赌场使用的筹码，置换成真实的资金套现出来，“远比你把房子卖了划算多了”。

老金听完，有些犹豫，心里盘算着这个提议的可行性和风险。见老金迟疑，樊某当场拿起手机，拨通了“某境外配资公司老板娘”的电话。对方信誓旦旦表示，自己有渠道可以与赌场内部关键人物合作，雇佣专业人士在网上娱乐平台或线下赌场进行洗码操作，平衡控制赌博输赢，相互配合将房产价值放大，共同牟利。“老板娘”还表示，只要老金愿意合作，她可以出具借条承担所有的亏损。

在一番“专业”的赌场术语下，老金虽然也没太明白其中的弯弯绕绕，但还是心动了。“我手上的房子大多是单身公寓，也卖不出什么高价，这个抵押套现倒是个不

错的投资方式。”他爽快地把市值近2000万元的14套房产的房产证复印件交给了樊某，并委托他前往澳门处理。还承诺事情办成后，给樊某一笔可观的报酬。

### 刷“码量流水” 刷走500余万元

然而套现之路，并没预期的那么顺利。两周后，樊某给老金打来电话，称想要套现更多的资金，还需刷上一波“码量流水”，营造一个“资深赌徒”的身份，来获取赌场的信任。

什么是“码量流水”？据樊某说，在赌场中，每次充值筹码都会生成一条“码量流水”，这相当于银行账户的进账记录，一定程度上能反映赌客的资金实力、赌博时长和押注大小等，是资产抵押套现的关键。

充值越多，流水越大，可套现的金额也就越多。

“想要赚大钱，前期的投入是必须的。”就这样，老金又转了10万元给樊某“走过场”，营造资深赌徒的假象。为此，樊某还特别向他出具了一张欠条。

之后的数周里，樊某需要“走过场”的钱越来越多。“凭我们这么多年的交情，他是不会骗我的。”老金犹豫了几次后，依然选择继续扩大资金投入，前后8次向樊某转账共计500余万元。

然而，好几年过去了，老金依然没能见到房产套现的钱，就连刷流水的500余万元，樊某也以各种理由推脱。在樊某的一次次失信中，本以为能血赚的老金这才醒悟过来自己被骗了，赶紧前往公安机关报警。

原来，樊某初中毕业后就步入社会，曾做过纺织、铝材料、农场等各种营生。可因为踏上了赌博这条不归路，最终债台高筑，于是动起了诈骗的歪心思。所谓的“抵押套现”“码量流水”，全是他结合赌博经验编造出来的。而给老金打电话的“境外配资公司老板娘”，其实是他的赌友。

目前，樊某虽然被警方抓获归案，但从老金处骗取的500余万元，早被他及身边的人赌博挥霍。近日，绍兴市越城区人民检察院以涉嫌诈骗罪对樊某依法提起公诉。目前，案件正在进一步审理中。

# 仅125秒银行卡就被复制了 揭秘新型信用卡盗刷案

新华社 毛鑫

拿到一个人的身份信息，仅用125秒，就可以“凭空”复制出他的信用卡。

广东广州警方最近公布的一起信用卡盗刷案，揭开集“重制、盗刷、销赃”于一体的新型信用卡诈骗犯罪内幕，警示了针对芯片信用卡的新风险。

### 125秒就能骗过银行 重制一张信用卡

“你好，我卡的芯片坏了，可以帮我补发一张吗？”

“请问预留手机号还在用吗？地址要改吗？请输入卡片的服务密码……感谢您配合。我给您重新寄张新卡过来。”

这是广州一家银行的客服电话录音。这通2分05秒的电话，竟牵扯出一宗跨多省份的新型信用卡盗刷大案。

2023年的一天，该银行向公安机关反映，银行客服短时间内突然接到大量要求重制信用卡的申请，情况异常。

该行信用卡中心欺诈风险管理部工作人员说，这些人打来电话，自称是该行客户，要求重制信用卡并修改信用卡邮寄地址。银行通过查验持卡人身份证号码和电话服务密码完成身份核对，按客户要求制作新卡。

“这些人收到新卡后，通过手机再次致电客服，验证卡片交易密码并激活，然后在外地大额刷卡购买黄金等。现已发现有6个客户的信用卡被盗刷，金额约61万元。”该工作人员说。

广州市公安局成立专案组。经查，该团伙自2022年10月至2023年3月间，共对7家商业银行的900余张信用卡展开攻击，成功补办信用卡500余张，成功激活并盗刷230余张，涉案金额1100万元。

该局经侦支队办案民警说，受害者受损金额少则1万元，多则10万元，“甚至有

的人信用卡被刷爆后，还被开通20多万元网贷”。

经过侦查，广州警方在海南、福建、江西等地抓获犯罪嫌疑人12名，解除潜在被盗刷风险金额超10亿元，打掉一个集“重制、盗刷、销赃”于一体的新型信用卡诈骗团伙。

今年4月，该案被公安部和中国银联银行卡安全合作委员会评为2023年“打击涉银行卡犯罪精品案例”。目前，检察机关已以涉嫌信用卡诈骗罪对涉案嫌疑人批捕起诉。

### 信用卡安全防线 是如何被攻破的？

本案警示针对芯片信用卡的新风险。办案民警表示，该团伙作案手法新颖，通过三招绕开了信用卡的安全防线。

——购买公民个人信息充当“破关弹药”。

该团伙通过“黑灰产”渠道购买大量公民信息用于盗刷。据主要犯罪嫌疑人刘某高供述，该团伙2019年花5000元通过境外社交群组购买了一批“料”，共计61万条公民个人信息，包括姓名、身份证号、信用卡号、手机号，及一串6位数字的密码。

有了“料”，还得有话术。“我冒充他人身份，跟银行客服说卡坏了、丢了，申请补办，然后变更收卡地址。”刘某高说，一般来说客服不愿意得罪顾客，会尽量满足需求；如果遇到有经验的客服不停地问，他就“爆

粗口”吓唬对方，最终成功几率接近50%。

——信号屏蔽、短信轰炸、呼叫转移三管齐下，防止卡主察觉。

为了让卡主忽略或收不到银行的短信提醒，该团伙先是冒充卡主身份，拨打通信运营商电话，开通短信屏蔽功能；此计若不成，就会购买短信轰炸服务，把银行提醒信息淹没在垃圾短信里。有的卡主对此毫无察觉，甚至警方取证时还被认为是骗子。

“在新卡快递派送时，开通卡主手机号呼叫转移，最终拿到新卡并激活。”刘某高供述，有时不得已也利用“电话回拨”软件，在银行客服处虚假显示为卡主原预留号码，以便顺利激活。

——领卡、盗刷、套现由不同的人分开操作，互不相识，通过虚拟币完成分赃。

据办案民警介绍，犯罪团伙买来社交媒体账号或者群组，发布“银行卡快钱工作”兼职信息，很快会有闲散人员联系上门，这些人被称作“车手”。不同的“车手”完成领卡、盗刷、套现，在扣除报酬后，换成虚拟币交给犯罪团伙。

“为了躲避侦查，犯罪团伙找A地的‘车手’，前往B地领取重制的信用卡，再到C地盗刷，最后通过虚拟币转账分赃。”办案民警说。

### 综合施策封堵漏洞

公安部不久前通报，2023年全国公安机关共破获伪造信用卡，窃取、收买、非法提供信用卡信息，妨害信用卡管理，信用卡



新华社 王鹏

诈骗、套现类非法经营等犯罪案件近5000起，涉案金额超百亿元。从一些公开的典型案例看，信用卡盗刷和非法套现等犯罪案件占比较大。

在办案民警看来，信用卡诈骗作案手段看似“巧妙”，究其根本还是钻了信息安全的漏洞，伪造身份进而层层突破防护网。广州市公安局经侦支队一大队二中队副队长李昀璁说，除了严打侵犯公民个人信息违法犯罪行为之外，还要提升群众风险防范意识，避免在生活中、网络上随意填报个人身份证、电话、支付账号、密码等敏感信息。

“有的密码设置过于简单，或者高度统一，作案团伙只要掌握其身份证号码或者其中一串6位密码，就可猜出其他重要密码。”李昀璁建议银行部门加强对用户的安全提醒服务，提醒群众对信用卡单独设置密码，并开通短信提醒功能，留意异常信息。

“治理信用卡诈骗犯罪需要多部门综合治理，这涉及各级职能部门，各大商业银行等传统金融机构和第三方支付公司、电商平台等。”广州市公安局经侦支队一大队二中队队长何浩建议，应加强警银企联系，依托“智慧新经侦”等技术平台，共同发力封堵漏洞、防范风险。

针对此案中发现的“补办新卡只需提交交易密码，不需要卡主预留手机致电”的情况，以及部分银行在信用卡安全防护上存在的漏洞，警方建议，银行升级信用卡安全防护措施，加强对客服人员的培训，以案说法，增强风险防范意识，依法依规办事，该拒绝办理的要明确拒绝。