近日，涉及国内多家银行数百万条客户数据资料、在暗网被标价兜售的消息广为流传。

尽管涉事各家银行进行数据比对核查之后，均否认了被兜售的数据资料包真实性。但是，牵涉面甚广的庞大的金融数据，尤其是银行用户涉敏信息的如何保障安全性，仍持续在行业引发关注、研讨。

尤其是，伴随银行线下业务线上化、与流量方边界日益拓宽等新变化，泄密在前端、在外包管理领域，也给银行数据安全管理带来新挑战。截至2019年底，我国开立银行账户113.52亿户、全国人均拥有银行账户数达8.09户，这些账户安全谁来守护？

这次疑涉百万条客户数据被盗卖的消息，神秘交易地“暗网”浮出水面，再次让更多人关注起这个通过特殊技术手段才可登入的秘境。

而更多人不知道的是，“你看到的只是冰山一角，暗网交易的信息非常非常多，金融相关信息可以占到7成以上。”通过连日多方采访，券商中国记者试图还原一组金融数据是如何被盗取、流入暗网、被谁交易售出、由谁流出市场的暗网链条。

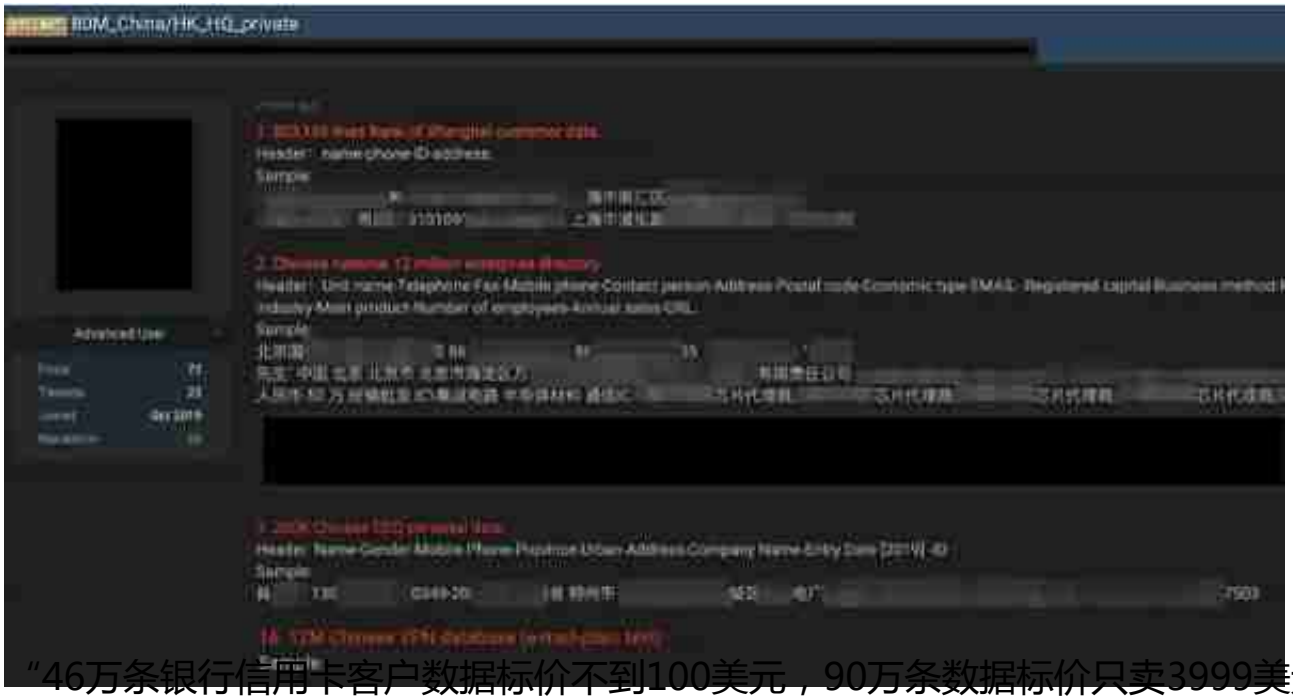
百万条用户资料被“白菜价”非法甩卖？

银行：与真实数据不符

涉及国内多家银行数百万条客户数据资料，在暗网被标价兜售，连日来引发行业广泛关注。4月15日，一位金融安全技术人士向券商中国记者证实了在暗网看到该条盗卖信息。

从数据安全人士此前发布的相关截图来看：被售卖信息里包含了大规模的金融机构客户数据泄露，其中涉及上海银行80.3155万条、浦发银行10万条、招商银行上海分行6.3万条、中国农业银行90万条、兴业银行46万条客户资料，其中既有储蓄账户、也有信用卡账户及私行理财账户，含客户姓名、客户类型、性别年龄、手机号码、开户账号、住址邮编、存款数据等信息。

此外，还包括经过初步分类的20万条企业代表资料，包含公司名称、注册资本、企业经营范围等。需指出的是，该部分信息多为公开可获取信息。



“46万条银行信用卡客户数据标价不到100美元，90万条数据标价只卖3999美元（折合人民币约2.8万元），简直是‘白菜价’；如果是真实数据，这么庞大的数据量实际售价至少10倍以上。”一位大数据行业风控总监向券商中国记者评价，尽管截图显示的样例数据非常详尽，但这么大的数据量价格却低得离谱，盗卖数据是不是真的、可信度要打个问号。

为了核实上述情况，记者也第一时间联系了涉事银行，各家银行相对一致态度是：经过核查比对，与真实数据信息不符；不排除不法分子将不明来源数据冠以金融机构名义兜售，以牟取非法利益。

兴业银行相关负责人回复，“所谓的‘兴业银行信用卡客户信息’与我行真实的客户信息要素并不吻合，不排除系不法分子伪造、售卖所谓银行客户信息牟取不当利

益。”

招商银行方面人士告诉记者，“经比对相关数据，与我行真实客户信息并不吻合，网络上的信息不属实。我行谴责任何伪造并贩卖公民信息的犯罪行为，并保留追究损害我行声誉法律责任的权利。”

浦发银行方面回应称，“经排查比对，相关数据无我行账户信息，且与我行客户信息要素不符。”

上海银行相关人士回应记者称，“进行了详细比对，发现其所谓客户信息中并无我行银行账户信息，且与我行真实客户信息关键要素并不匹配。可认定该贩卖信息非我行泄露数据，不排除系不法分子为牟取不当利益伪造、拼凑、出售所谓银行的客户信息。”

全国开立银行账户达113.5亿

谁在守护安全？

百万条被兜售的数据资料包尽管真实性被驳，但庞大的金融数据尤其是银行用户涉敏信息的安全性如何保障？已足够引起行业及监管对金融数据安全的重视。

央行统计显示，银行账户数量稳步增长，截至2019年末，全国共开立银行账户113.52亿户、同比增长12.07%，其中，全国开立单位银行账户6836.87万户、同比增长11.73%，个人银行账户112.84亿户，同比增长12.07%，全国人均拥有银行账户数达8.09户。

为业界所公认的是，金融行业尤其是银行业是风控建设最好的行业，其中信息科技领域的风控建设和落地水平远高于其他行业。依据银保监会“商业银行信息科技风险管理指引”，银行业有严格的风控建设体系和风控监督体系，有严谨的风险控制点的识别、评价、处置、跟踪机制。

“银行业信息科技风控要求较高，需要符合国内外风控管理要求，包括商业银行信息科技风险管理指引、巴萨尔协议、塞班斯法案等。”腾讯安全数据安全团队负责人彭思翔告诉记者。

杭州某大型技术公司金融事业部总经理曾负责过银行物联网解决方案，涉及到数据服务采集业务，他向记者举例，“设备采集的信息一般会保存在当地银行机构，在信息保存、传输安全性方面，一方面是，银行本身设有专网，内网、外网隔开，还有硬件设施方面的防火墙设置防护；另一方面，各家银行内部有各个层级对安全认

证的严格复核管理。”

“银行的IT系统不具备大规模向外泄露数据的可能性。”一家股份行风险管理部门总监向券商中国记者分析，“按银保监会的相关规定，银行业IT系统基本分为：生产域、测试域、互联网域等，其中，三个域之间的数据传输收到严格限制。只有在生产域才能看到数据的全貌，测试域只有用于测试的数据，有数据量和脱敏的相关要求，互联网域基本没有客户信息。从技术上、系统上，大规模数据外泄讲不通。”

DataVisor黑产研究专家、高级技术经理周君桢的看法类似，金融机构尤其是银行的安全风险等级最为严格，一方面是监管要求高、管理严；另一方面是业务属性决定，对于银行来说，客户账户信息是核心商业价值要素之一，银行会投入大量人力、物力做相关保障，大中型银行也具备强大技术团队和实力。

流量经济爆发的安全新挑战：泄密在前端

从近期发布的国有六大行年报来看，其中有四家2019年科技投入总金额突破百亿元，最高的建设银行投入176.33亿元；截至2019年末，工商银行金融科技人员规模多达3.48万名、在全员占比高达7.82%，其次是建设银行、交通银行、中国银行、农业银行金融科技人员占比分别为2.75%、4.05%、2.58%、1.58%。

银行加大科技投入、科技人员扩容规模空前。然而，银行数据涉密各个环节，尽管被最高等级的风险防护，仍难有万全之说。

首先是不同金融机构之间、金融机构内部之间的安全能力有差异。“大中型的金融机构风险等级高，但是一些分支机构风险能力就较弱，可能账户密码保护不严密。一些地下灰黑产业，就会有组织、有目的性地去攻击，抓住一些系统平台存在的漏洞。”周君桢介绍。

“银行的风控水平并不是一碗水端平。”上述股份行智能风控中心总监直言，“有的银行风控水平高、有的银行风控水平低，实力强的银行所有的模型都是行内专业人员建模；但是对于部分地方偏远地区的银行等，缺乏高端数据专业人才，只能通过外包方式去建模型。甚至部分不具备技术能力的银行直接拿过来就用一些第三方公司流量数据，这些数据包括身份认证三要素和部分行为特征，但是往往这类数据可能在使用前已经可能被泄密了。”

“泄密环节出在前端。”——在数位金融机构风控资深从业人士看来，这是伴随着近几年的银行线下业务线上化，在风险防控上一个更应该引起行业注意的新变化。

在彭思翔看来，银行数据泄露可能发生的场景，除了信息科技运行领域访问控制策略不当，开发、测试和维护领域三个环节未分离或分离后数据未脱敏，以及信息安全领域系统漏洞之外，其中一个重要的方面就发生在“外包管理领域”，“特别是对外包研发、测试的管理不当。生产环境暴露、数据库过度授权，都会引起数据泄露。”

“因为行业业务属性不同，银行的IT系统和互联网公司之间，往往有代际差异。”该股份行智能风控中心总监向记者举例。“比如面对一个互联网流量平台采用流量分发模型，100万客户分发给数十家不同的银行，与之相应的，银行与之对接的是流量准入模型；很天然地，这两个模型之间是对抗关系，准入模型希望准入更多，而分发模型希望筛掉更多；在现实情况中，相比互联网公司，银行IT系统灵活度、可使用工具、覆盖的行为数据数等，都处于相对劣势。”

“今后银行数据风控管理必将趋严”

“为促进金融行业健康发展与风险控制，监管层已经通过发布监管指引并将数据治理与监管评级挂钩的方式，来提高银行业对数据治理工作的重视，不管有没有出现这次的事件，银行今后数据风控管理上必将是趋严的。”数位银行业内人士均认为，尽管这次盗卖数据真实性存疑，但它后续仍然会也业务层面产生影响。

2018年5月，银保监会发布《银行业金融机构数据治理指引》，旨在引导银行业金融机构加强数据治理。去年12月，金融业移动金融APP备案首批试点开启，首批23家试点备案名单中就有16家银行，含5家国有大行、5家股份行、3家城商行、2家农商行、1家农信联社，涉及提升安全防护、加强个人金融信息保护、提高风险监测能力、健全投诉处理机制、强化行业自律5个方面，并划定了涉及个人金融信息采集、使用、留存等方面四大红线。

事实上，银行数据管理趋严背后，是国家层面对个人信息数据管理工作地系统性出击。去年下半年，工信部等数次公开点名批评百余款应用软件及其运营企业，涉及未经用户同意超范围及非必要使用个人信息等违规情形。

券商中国记者注意到，去年5月份到8月份，监管部门密集出台了关于数据安全管理办法、APP违规收集使用个人信息行为认定方法等多项征求意见稿及草案。这也和上述数位银行业人士的判断类似，当前央行对银行数据治理指引已经非常详尽，未来的变化更多出现在相关立法层面。

“在数据确权、数据治理上，中国有着绝对的优势，将是一个世界性的数据资产大国。”京东数科数字技术中心数据资产部总经理张旭认为，数据资产是银行的核心资产，是政府安保数据之外最值得信赖的数据，但数据向前发展必然面临着确权，

以及海量数据在手之后如何通过人工智能等新技术做深度挖掘、开发应用。

“从大环境的导向来看，为业内普遍认同的是，监管曾仍然鼓励在合规前提下推动金融机构数据高质量发展，比如与各类政务数据互联互通，建立跨区域的数据融合应用等。”苏宁金融研究院院长助理薛洪言接受券商中国记者采访时称。

庞大数据黑色交易网：金融相关占比7成以上

“暗网售卖数据是有组织严密的产业链，窃取售卖数据是黑产中隐藏最深的、历史最悠久的、最成熟的变现方式。”腾讯安全数据安全团队负责人彭思翔直言。

2018年被业内认为是数据保护的元年，却也是数据泄露的灰色之年。当年3月，Facebook被曝8700多万条用户数据泄露、遭遇其有史以来最大型数据泄露危机。而在国内，2018年初有国内某评价连锁酒店传出涉及5亿条顾客隐私数据在暗网贩卖；今年3月，国内某APP发生信息泄露，在暗网上被以“5.38亿用户绑定手机号数据，其中1.72亿有账号基本信息”的名义进行售卖。

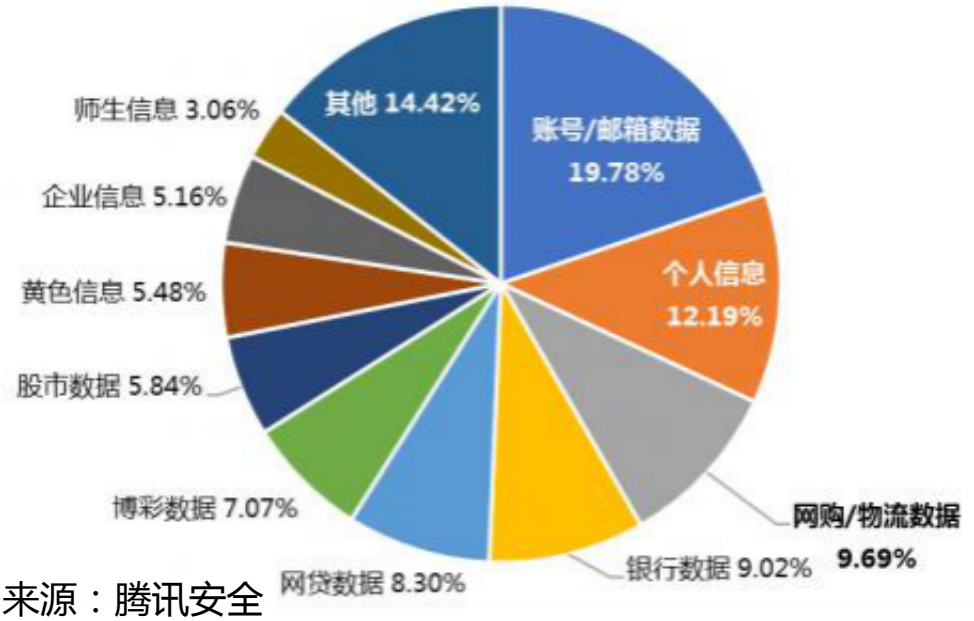
近年来频繁爆发重大企业信息资料或用户数据泄漏事件，让暗网这个“地下黑市”逐渐被社会所认知。

“暗网，可以简单理解为互联网的一个地址，有一定技术手段都可以访问。最大特性是匿名平台，很难追溯，匿名传输，匿名货币交易。”周君桢告诉记者，“市场规模很难统计，你看到的只是冰山一角，暗网交易的信息非常非常多。”

而他注意到一个明显的变化是，从2018年以来，随着传统金融数字化转型的加速，银行、证券、保险尤其是互联网金融等类型金融数据明显增多，诸多信息经常在暗网上被倒卖，
“金融相关的数据情报数据占到7成以上，尤其涉及金融属性的个人隐私信息，如金融开户信息，信用卡等，国内国外同样如此。”

腾讯安全报告从2018年暗网数据交易的情况（抽样数据）来看，帐号/邮箱类数据、个人信息、网购/物流数据、银行数据、网贷数据位列前五，分别占比为19.78%、12.19%、9.69%、9.02%和8.3%，其它还有博彩数据、股市数据、企业工商数据等信息。

2018年暗网交易数据分布占比情况



来源：腾讯安全

彭思翔介绍，黑产者盗取数据的具体手段包括技术入侵、社会工程学及APT攻击，也形成了脱、洗、撞三步循环的模式，“脱库是指入侵有价值的企业，把数据库全部盗走；洗库指对数据初步清洗，拿到其中最有价值的数据去变现；撞库指清洗后发现可以继续利用的数据，会到别的应用、企业继续尝试渗透脱库，形成循环操作模式，一个企业或者一个行业的数据将全部被获取。”

比如，银行业里储存了大量用户敏感信息且又全又准确，而银行开展了大量业务应用、更新速度快，这又带来攻击面大、窗口多，但银行又很难做到滴水不漏的防护，“这就会成为黑产重点攻击的目标。”

由谁卖出、被谁买入

不少人有类似的经历：在某银行刚办理按揭贷款，随后不断收到各类第三方平台的信贷类、消费类营销电话和短信。

“这是典型的个人信息泄露的情况，比如房贷办理需书面填写较多个人信息，不排除有机构人员或信息接触者将信息留存在转手倒卖，比如一些信息中介或金融代理机构，联合第三方营销推广平台的惯用操作手法。”周君桢解释，“不过，相比这类信息泄露，暗网更多是有组织、有目标的盗取、买卖。”

“早期一般一个团队或者单人来完成，但是目前已经完全产业化、专业化，固定的团队进行脱库，再卖给洗库团队，再卖给撞库团队，互不干涉，通过虚拟化货币交割，追查极其困难。”彭思翔告诉记者，“绝大部分被盗数据不会公开出来，而是进入到秘密交易环节，作用在特定的场景中，如竞争对手战略分析、同业用户争夺

、上下游业务定推等，此类秘密交易也可称为定制化数据交易，特点是数据只卖一次或在某个时间窗口禁售，而公开在暗网交易的数据是多次多家进行贩售。”

而在买方上，“更多不是在个人论坛卖，往往是卖给专业信息商或数据商，后者对数据加工、匹配、拼接，数据完整性会更好，层层转包、价值会更高。”周君桢介绍，通过数据加工完善，信息精准度明显提高，国内的电信诈骗、国外的信用卡盗刷往往由此。

另一特征是其全球化趋势，全球都存在数据黑产，且成为数据跨境非法流动的主要渠道。“如非洲国家的个人信息，被不法代理用于亚马逊用户注册，进行欺诈和作弊行为。”彭思翔介绍，黑客会把数据进行整理并相互交流、形成黑产的大数据服务商，具体来讲就是社工库，在利益的驱使下，黑产向大数据服务和基础设施建设等大规模、高技术发展，这也给数据安全的治理加大了挑战难度。

三大变现途径：精准诈骗、撞库攻击、撒网式诈骗

截至2019年末，中国网民数达8.29亿，手机网民规模达到8.17亿，在网民总数中的占比提升至98.6%；数字经济渗透在社会生活方方面面，个人的数据轨迹也无处不在。

暗流涌动的黑市交易侵蚀着用户隐私，而被盗取贩卖隐私数据在直接变现以外，黑产从业者往往还会被利用购得数据进行精准诈骗等犯罪行为，进一步损害个人权益。

腾讯安全报告统计，信息泄露催生三大变现途径：精准诈骗、撞库攻击以及撒网式诈骗。

一个写在腾讯安全报告的案例是，网购用户买完东西后，收到热心“客服”的电话，“客服”以质量问题、物流问题等事由，发送一个退款网页链接或二维码，用户按照提示操作即可退还高于购物款的退款或退款保证金，之后“客服”会进一步引导用户把多收到的钱退还给网店。

而很多人不知道的是，这是诈骗者通过暗网等获得网购用户详细信息后进行的针对性电信诈骗。用户收到的款项其实是一些正规的贷款平台的快速贷款，诈骗者利用网银或第三方支付平台上快速授信贷款等服务，误导用户从贷款平台贷款、然后将“多余”的款项打回诈骗者的网络帐户。

段久惠

证券时报·券商中国记者，专注银行、支付、金融科技、大资管领域资讯和人物采写。力透纸背，记录资本风云、大历史众生百态，是吾志趣。你有往事，我有笔墨；坐标上海，欢迎交流。

重磅信号现身，A股可稳？俩老头周末震动全球，五位大佬大举做多，有企业主却疯狂买楼，发生了什么？

最新！全球确诊232万，美国超73万，欧洲超108万！印度再现群体感染，哈尔滨惊现1传50，首现医生被感染

10倍配资、国家认证资质...统统是谎言！警方侦破特大荐股诈骗案，虚拟盘诈骗2000多万，同花顺借机证清白

懵圈！油价跌至负数？竟有原油生产商白送还"包邮"！全球最大商品交易所也在改软件，支持负油价交易

4天暴涨93%！可转债炒作卷土重来？日均换手28.7倍，投资还是投机？监管正密切关注

券业巨变？券商开户导流烧至今日头条，低佣金战火再起？两家合作券商火速删除佣金信息，字节跳动也回应