征信查询前置系统的信息安全防控研究

杨帆
杭州坤泽实业股份有限公司
DOI:10.12238/acair.v2i2.7359

[摘　要] 现代社会下,发达的网络社会和丰富的经济活动推动着社会信用体系日渐完善,使得信用信息也逐步成为人们关注的一项重要信息。如今我国已建立统一的金融信用信息数据库,其中收录了大量个人、企业及其他组织的信用信息,促进了征信领域发展的同时也带来了极大的信息安全压力。征信信息具有高敏感性,密切关系到个人生命、财产安全,一旦泄露将对个人及社会造成严重损害。征信查询前置系统是连接信用信息数据库及WEB应用界面的重要系统,加强相关管理和防护工作对于维护征信信息安全具有重要意义。本文对征信查询前置系统的信息安全风险及安全防控的必要性进行简单分析,并探讨具体的安全防控措施。
[关键词] 信息安全；征信查询前置系统；防控措施
中图分类号：F062.5　文献标识码：A

Research on information security prevention and control of credit investigation pre-inquiry syste

Fan Yang
Hangzhou Kunze Holdings Co., Ltd

[Abstract] In modern society, developed network society and rich economic activities promote the improvement of social credit system, credit information has become an important information people pay attention to. Nowadays, China has established a unified financial credit information database, which includes a large number of credit information of individuals, enterprises and other organizations, which promotes the development of the field of credit investigation, but also brings great pressure on information security. Credit information is highly sensitive and is closely related to the safety of personal life and property. Once leaked, it will cause serious damage to individuals and the society. The pre-credit inquiry system is an important system connecting the credit information database and WEB application interface. Strengthening relevant management and protection work is of great significance to maintain the security of credit information. This paper briefly analyzes the information security risk and the necessity of security prevention and control of the pre-inquiry system, and discusses the specific security prevention and control measures.
[Key words] information security; credit inquiry front system; prevention and control measures

引言

近年来,我国企业征信系统、个人征信系统在不断完善,广泛收集企业、个人的信用记录,建立征信数据库,为金融活动提供征信信息支持,以尽可能地降低金融交易风险。随着各类信用贷款的发展,征信信息的应用越来越广泛,受到的关注度也不断增高,社会对征信记录查询服务提出了更高的要求。为了便于企业和个人的征信查询,中国人民银行分支机构及部分商业银行代理查询网点向社会提供征信报告查询服务[1]。而该服务较为复杂,涉及面较广,其中许多环节能够获取用户敏感信息,在为社会提供便利的同时也带来较大信息安全风险。如何做好征信信息安全防控问题成为相关领域关注的重点,迫切需要加强相关防控技术的应用,采取有效防控措施。

1 征信信息安全防控的必要性

随着信用体系不断完善,征信范围逐渐向金融以外的领域延伸,社会对征信报告查询服务的需求显著提升,其中暗含的信息安全问题也越来越严峻。征信查询前置系统是连接征信系统数据库和WEB应用系统的预处理系统(如图1所示),需要对用户查询授权资料进行预审核,确定无误后才能访问征信数据库,其中涉及到大量的高敏感信息数据,包括用户个人身份信息、征信记录、证件照片等。在大数据时代下,这些敏感信息具有很高的价值诱惑,促使部分不法分子采用各种手段进行窃取、滥用。部分征信查询服务平台或个人在利益驱使下,违规出售个人信用

信息以获取高额利润,扰乱了征信市场秩序,危害信息安全[2]。近年来,个人信用信息泄露案件屡屡发生,数量不断增多,导致信用信息主体的个人合法利益受到严重损害,带来恶劣的社会影响,增加了社会群众内心的不安全感,破坏了征信市场应有的秩序,对社会发展造成不利影响。信用信息泄露还可能引发金融犯罪,甚至增加金融危机的风险,维护征信领域信息安全是防范金融风险的重要手段。因此,很有必要加强对征信查询前置系统的管控,制定适宜的信息安全防护策略,以促进征信行业的健康、有序发展。

图1 征信数据管理系统结构

2 征信查询前置系统的信息安全风险

随着社会经济发展,征信活动的活跃度不断提升,信用报告查询量也随之增多,要想有效保障征信查询前置系统的信息安全,必须要明确具体的风险点。威胁征信信息安全的风险类型主要有以下几种:一是内部人员借助职务之便非法查询征信信息、非法获取征信报告。社会对征信查询服务的需求扩大,催生出了更多的征信查询服务平台和网点,相关工作人员也随之增多。部分内部人员的工作中能够触及到征信信息的查询操作权限,包括部分系统管理人员、业务操作人员等[3]。若人员法律意识、职业道德意识不够强,就可能在利益驱使下与不法分子勾结,利用内部查询账户批量盗查征信数据库中的信息。部分内部人员还可能通过拍照、截屏、本地下载等方式非法获取征信报告,危害用户的征信信息安全。二是外部不法分子利用网络攻击手段侵入征信查询前置系统的传输网络和服务器中,非法窃取其中的敏感信息,包括征信信息主体姓名、联系方式、证件号、证件照片、征信记录、授权信息等,导致信息泄露[4]。此外,不法分子还可侵入自助查询终端,批量查询、提取大量人员的征信记录和个人敏感信息,对信息主体的利益造成损害,威胁征信行业和社会整体的和谐稳定发展。

3 征信查询前置系统的信息安全防控措施

要想更好地保障征信系统信息安全,需要分析、梳理可能造成征信信息泄露的风险点及原因,针对性提出有效防控措施,找出薄弱环节并进行弥补、加强管控,建立完善的安全防控体系,从而有效堵住漏洞,降低征信信息泄露的风险。

3.1系统访问控制

为了有效防控来自外部的网络攻击,防止不法分子通过各种技术非法访问系统,窃取信息数据,相关部门要加强对征信查询前置系统的访问控制。首先,应在征信查询前置系统与征信系统之间增设一道防护墙,屏蔽其服务器地址、用户名、密码等,防止外部网络不法分子利用网络漏洞发起攻击,导致敏感信息泄露。为了保证信息传输安全,应在征信查询前置系统中合理运用信息加密技术,对征信报告、个人信息、证件照片等敏感信息采用HTTPS加密传输,防止信息在传输过程中被不法分子窃取。其次,可通过绑定用户和客户端IP地址的方式降低非法访问风险。将用户和查询设备绑定后就只能通过用户本人所使用的那个设备登录征信查询前置系统,从而有效防止用户本人以外的人非法访问征信系统,查询其个人征信信息[5]。最后,要加强网络安全防护,确保征信查询前置系统处于安全的网络环境中运行,降低信息泄露风险。应当在金融内网中部署征信查询前置系统,与外网实现物理隔离,并加强防火墙建设,增强网络对外部网络病毒、黑客攻击的抵御能力。可通过设置“白名单”的方式合理控制访问权限,确保只有“白名单”上的IP地址才能登录、访问征信查询前置系统。

3.2用户管理

针对外部人员非法登录和内部人员非法查询征信信息的问题,要加强对用户的管理与控制,要求所有查询用户必须实名制,对其个人身份信息进行审核、登记,确保是本人进行征信查询操作。征信查询前置系统运行过程中能够接触到敏感信息的主要有两类,即管理人员和操作人员。负责系统管理的人员具有用户管理、角色设置、核查管理、权限管理等方面的职责和权限。业务操作人员的工作则涉及报告查询、异议声明处理等内容,能够直接接触到用户的征信信息。征信查询前置系统可对用户进行分级管理,各级用户设置不同的权限,在满足职务需要的基础上,尽可能地减少内部人员的查询权限、管理权限范围。在管理系统中,依据用户权限划分不同角色,包括各级管理员、核查员、查询员、异议声明处理员等角色,只有最高级别的管理员能够进行角色设置和权限管理,包括新增角色、删除角色、设置角色权限等。尤其需要注意管理权限和操作权限不能重叠,两种职位不能由同一人兼任。

3.3在线核查

各级征信报告查询机构、网点需要定期对用户进行在线核查,可以月、季、年为单位进行阶段性抽查,按照一定比例随机抽取企业、个人的查询记录进行在线核查。为了提高效率,应规范在线核查的具体流程,由系统自动抽取历史查询业务作为核查样本,由专业核查人员进行线上核查、线上标记,并自动生成电子台账,其中涉及核查人员、核查时间、核查结果等工作详情,为相关监督、管理工作提供依据。抽取样本时,核查人员可在系统上选择抽查时间范围、用户类型、查询机构、查询业务等条件,并设置相应的抽查比例,由系统依据条件自动生成核查样本,从而有效提高样本准备的效率,降低人为操作失误带来的风险

和误差。核查人员需要对每一条个人或企业的征信查询记录和授权资料进行核实，输入核查结果，若该笔查询业务存在异常，则输入异常结果后自动发送到相关查询员处，进行进一步审查核实。核查完成后系统自动在查询业务记录上添加“已核查”标记。

3.4异常行为监测

异常行为监测是指对征信查询前置系统中的查询行为进行实时监测和分析，以便于及时发现异常行为信息，察觉可疑操作，及时发出警报并阻断其查询操作行为，从而降低损失，防止征信信息被窃取。管理人员接收到系统警报信息后需及时进行核查，若无异常则对被阻断查询操作的用户进行重启。征信查询前置系统中有以下情况时可识别为异常行为：(1)查询量激增：单日查询量异常增高的情况下，可能有征信信息泄露的风险，可通过分析过往的日均查询量、月均查询量，设置合理的报警参数阈值和阻断参数阈值，对系统征信报告查询量进行自动监控，一旦查询增量超出安全阈值则自动触发系统警报甚至触发自动阻断操作。当管理人员接收到报警信息后，需及时进行核查和处理，确保征信查询前置系统的信息安全。(2)睡眠用户重启：长时间未使用的用户重新登录查询时也可识别为异常行为，可通过后台设置具体的连续未登录天数，当超出一定时间内未登录的用户重新登录后，系统自动发出警报信息，提醒管理人员留意。(3)查询失败比例过高：当用户当日查询失败次数过多，与总查询量的比例超出一定阈值后，也可触发系统的异常行为报警，将其标记为可疑查询行为。(4)异地查询量过大：若当日系统中的异地用户查询数量超过一定的比例，则具有一定的信息泄露风险，应在征信查询前置系统中设置异地登录、异地查询的安全阈值，若比例过高，则要分析、检查有无可疑查询行为。

3.5敏感信息的防护处理

征信查询前置系统运行时涉及到大量敏感信息，包括用户个人信息、授权资料、查询日志等，其中蕴含着巨大的价值，容易成为非法分子的目标。为了保证此类敏感信息的安全，有必要采取适当的防护处理措施。例如，征信报告展示页面中只展示首页基础信息，无法直接查看完整、具体的征信记录，并禁止在此页面使用截屏、另存等操作，防止征信报告被非法查询、非法获取。展示有用户姓名、照片、证件号等敏感信息的页面需要设置水印，标明系统时间、登录用户名等信息，以便于后续出现信息泄露问题后能够有效追踪信息来源。征信查询前置系统的日志记录中，对于用户姓名、证件号等敏感信息应屏蔽显示，一律用“*”号替代，防止不法分子通过系统日志记录大批量获取用户敏感信息。最后，要确保敏感信息数据的储存安全，敏感信息要加密储存，授权资料不能储存在任何查询终端设备中，而是全部传输到人民银行的储存服务器进行统一储存。

3.6完善管理机制

科学的管理机制对于维护征信查询前置系统信息安全有着重要作用。相关部门要全面分析征信报告查询过程中的薄弱点和风险点，加强相关管理和控制，以降低信息泄露风险。例如，部分人员通过重复打印的方式非法获取用户征信报告，因此需要完善对报告补打操作的审核，使客户端查询到报告后只能点击一次“打印”按钮，若需要二次打印，则必须提交补打申请，由专人审核无误后方可打印。在授权资料补录、司法查询等方面也是同理，需要由专人复核相关资料后即可进行操作，以确保信息安全。为了防止内部人员借助工作之便非法查询征信信息、获取征信报告，应加强对内部人员的管理。在征信查询前置系统中设置工作时间，使内部人员只能在工作时间内使用查询账户登录，并加强人员操作时的监督，防止内部人员通过拍照、下载、截屏、打印等方式非法保存用户的征信报告。除此之外，还要加强对自助机的管理。随着征信报告查询自助机设备越来越多，给广大用户带来便利的同时也带来一定的安全隐患，应将所有查询自助机均纳入查询前置系统进行统一管理，设置设备自动开机、关机时间，并从多角度进行日志管理，包括操作日志、管理日志、系统日志等，记录自助机工作情况，做到一切操作都有迹可循，防止不法分子趁着无人看守侵入自助机盗取信息数据，威胁信息安全。

4 结语

随着征信系统的普及，确保征信查询前系统的信息安全性变得尤其关键。为构建一个全方位的安全防护体系，必须从系统访问控制、用户管理、在线核查、异常行为监测、敏感信息防护处理以及完善管理机制等多方面着手，如此方能有效预防来自内部和外部的信息安全威胁，确保个人和企业征信信息的安全性，维持征信市场的正常运行，并推动社会信用体系朝着健康的方向发展。

[参考文献]

[1]贺小琳.征信查询前置系统信息安全防控策略探析[J].征信,2022,40(07):51-55.

[2]崔琳琳.组织行为视角下的征信信息安全监管机制研究[J].时代金融,2020,(03):110-111.

[3]皮文爽.金融信用信息基础数据库接入机构征信信息安全风险技术防控路径及优化策略[J].财经界,2021,(2):176-178.

[4]柴亮.基于征信查询前置管理系统的设置与实现[J].甘肃科技纵横,2020,49(03):7-9+70.

[5]崔琳琳.组织行为视角下的征信信息安全监管机制研究[J].时代金融,2020,(03):110-111.