互联网交易网络保安检视

证券及期货事务监察委员会（「**证监会**」）已发布报告及于2020年9月23日发出通函（「**该通函**」），详细阐述2018年7月生效的《降低及纾减与互联网交易相关的黑客入侵风险指引》中规定的监管要求。本注释概述了上述关于互联网经纪行应为流动交易应用程序采用的特定系统保安监控措施的事实调查结果及指引。

系统登入适用的双重认证

不足之处	证监会提出的措施
• 容许客户解除系统登入的双重认证功能 • 经电邮传送一次性密码作为第二认证元素的做法并不可靠 • 与绑定客户装置有关的问题，例如技术性保安漏洞，或容许客户绑定过多装置	• 不应容许客户解除系统登入的双重认证功能 • 不应经电邮传送一次性密码 • 应定期进行技术评估，以识别保安漏洞 • 不应容许客户就其互联网交易帐户绑定或注册过多装置，及应就并行登入（concurrent login）实施监控措施

侦测未经授权接达的监察及监督机制

不足之处	证监会提出的措施
• 某些大型互联网经纪行只对客户交易进行人手检视 • 只不定期、按周或按月进行监察及监督 • 自动化互联网协定（internet protocol，简称IP）地址监察工具的设计有缺陷	• 应顾及互联网交易业务的规模，并实施就业务需要而言属适当及相称的监察及监督机制 • 应至少每天进行监察及监督 • 应在实施自动化的IP地址监察工具前进行充分的技术测试及使用者测试

数据加密

不足之处	证监会提出的措施
某些公司没有充分地加密及保护客户登入数据、密码及交易数据，因为它们所实施的加密程序并不符合国际保安标准	互联网经纪行应持续检视国际保安标准，查核其数据加密程序的状况，及在适当时将其升级

网页超时

不足之处	证监会提出的措施
• 网页超时监控功能可被客户关掉 • 网页超时的时限可长达24小时	• 不应容许客户关闭网页超时监控功能 • 互联网经纪行应限制闲置超时时限（例如在30分钟以内），但须事先作出评估及持续进行监察 • 互联网经纪行应进行充分的测试，以确保网页超时监控措施妥为设定及运作

遥距连接的保安监控措施

不足之处	证监会提出的措施
某些供货商获授予随时适用的永久的遥距接达权，因而增加了网络保安风险。	互联网经纪行应避免向外界人士授出永久的遥距接达权

网络保安管理及监督

不足之处	证监会提出的措施
许多公司没有在其信息科技审计或自我评估中充分涵盖有关的基本规定	互联网经纪行应至少每年在其信息科技稽核或网络保安评估中检视其遵守基本规定的情况

流动交易应用程序

不足之处	证监会提出的措施
• 未能侦测并阻止被破解的装置登入互联网交易系统 • 没有充分地保护原始码，使黑客得以绕过内置的保安监控程序 • 流动交易应用程序中存在没有使用的程序代码库或模块，增加了黑客安装恶意软件的风险 • 容许客户的敏感数据储存在流动装置内，及有关数据不会在注销后从系统进程内存中被删除，从而增加了有关数据被黑客存取的风险 • 容许在没有妥善验证的情况下，修改储存在客户流动装置内有关该客户的生物特征数据，及没有在多次登入尝试失败后停用生物特征认证	• 应侦测及阻止被破解的流动装置登入互联网交易系统 • 应模糊原始码以加强保护，避免其遭恶意利用 • 应将没有使用的程序代码库或模块从原始码中清除 • 应在客户一旦离开安装于其流动装置的互联网交易应用程序或注销其互联网交易帐户后，便将客户敏感数据从有关程序中清除 • 互联网经纪行应收紧生物特征认证的保安监控措施，例如：- o 规定客户生物特征数据的任何改变须接受核实检查；及 o 限制认证失败的次数

鉴于该通函主题事项的技术性质，互联网经纪行应按需要向其供货商及其他顾问寻求专业协助。

如有进一步咨询，请联络本律师行杨元建律师（电话：(852) 2854 3070 或 电邮：lawrence.yeung@ycylawyers.com.hk）。

本注释并非也不应被视为法律意见。如有任何疑问，请就具体个案咨询法律顾问。

2021年2月24日