

常见问题与解答（更新于 2021 年 4 月 27 日）

常见问题与解答

学校网站可能看上去与您上次访问时有一点不同。我们目前正在进行添加和上传常见问题与解答清单的工作，并且将继续在有更多可用信息时将新信息包含在内。

您可 [here](#)（在此）注册获得信用监测服务。如果您已经注册，则无需为激活您的监测采取任何其他行动。

1. 发生了什么？

2020 年 12 月 24 日，Accellion 的文件传输应用程序（FTA）成为一次国际攻击的目标。犯罪者在此次攻击中利用该应用程序的弱点，攻击了包括大学、政府机关和私营公司在内的 100 多家组织。由于此次攻击，某些大学的数据在未经授权的情况下被访问。我们于 2021 年 3 月 29 日发现这些数据中的部分数据被发布在互联网上。

学校很重视隐私和安全，目前也在改善保障和保护学校信息和系统的措施。学校已经停止使用 Accellion FTA，目前正在向更加安全的解决方案过渡。学校目前正在与 FBI 配合，并且与外部网络安全专家合作，以调查此次事宜，确定具体发生了什么，有影响哪些数据，以及这些数据的所有人。

2. Accellion 数据外泄有影响哪些人的信息？

虽然调查工作还在进行中，但有证据显示未经授权的当事人得以访问的文件包含学校社区成员的个人信息，包括员工和他们的受抚养人、退休人员 and 受益人、捐献者、和目前是以及有望成为学校的学生。

学校目前正在努力确定哪些社区成员的个人信息受到影响，以及他们的联系信息。这些调查工作需要时间，我们也在一步步认真工作的同时，尽快提供准确的信息。在未来 45 到 60 天内，我们预期会向个人信息有受到影响、学校也有他们的当前联系详情的人发送恰当的个别通知。

3. 受影响的信息类型有哪些？

受影响的信息可包括全名、地址、电话号码、社会安全号码、驾照信息、护照信息、财务信息（包括银行路由和账户号码）、保健和相关福利信息、残障信息和出生日期，以及其他个人信息。

学校目前正在努力确定哪些社区成员的个人信息受到影响，以及他们的联系信息。这些调查工作需要时间，我们也在一步步认真工作的同时，尽快做到提供准确的信息。在未来 45 到 60 天内，我们预期会获得我们需要的信息，以向学校有他们的当前联系详情的人发送个别通知。

4. 我需要做什么吗？

学校目前通过益博睿（Experian）IdentityWorks 提供免费的监测和身份盗窃保护服务；点击 [here](#)（此处）注册。

我们请学校社区的成员做到一直对身份盗窃或欺诈等威胁保持警惕。除此之外，对“网络钓鱼”电子邮件，或者来电人表现出一副他们认识您的样子或声称是您可能有业务往来的公司的一部分的电话，以及让您提供敏感信息（例如密码、社会安全号码、财务账户信息等）的要求等提高警惕，总是一个好主意。您可将疑似网络钓鱼或试图实施社交工程诈骗的报告发送至 communications@ucop.edu。

我们还建议您为有提供多因素验证的在线账户设置此类验证流程。

关于获得免费的信用报告的信息

依照美国法律，美国居民有每年从三大征信机构中的各家获得一份免费信用报告的权利。如要获得您的免费信用报告，可访问 www.annualcreditreport.com 或拨打免费电话 (877) 726-1014。

关于执行欺诈警报或安全冻结的信息

您可使用下文给出的地址联系三大征信机构，以在您的信用报告上设置为期一年的免费欺诈警报。欺诈警报会向任何请求获得您的信用档案的人显示您怀疑自己可能是欺诈的受害者。欺诈警报不会影响您获得贷款或借款的能力。该警报只是会警示企业您的个人信息可能已被泄漏，需要该企业在为您发放借款前核实您的身份。如果您是借款的申请人，这可能会导致一些短期延迟，但这么做可能会保护您，以防他人使用您的姓名获得借款。

除了欺诈警报外，您还可考虑在您的信用报告上设置免费的安全冻结。安全冻结会禁止信用报告机构在没有书面授权的情况下透露消费者信用报告中的任何信息。还请您注意，在您的信用报告上设置安全冻结，可导致您为获得新的贷款、借款、抵押贷款、就业、住房或其他服务提交的申请的及时获批有延迟、被干扰或阻止。信用报告机构可能不会针对设置、暂时取消或永久撤销安全冻结向您收取费用。

如要在您的信用报告上设置欺诈警报，您必须联系下列三家征信机构中的一家，其余两家会自动添加欺诈警报。如要在您的信用报告上设置安全冻结，您必须联系下列三家征信机构中的一家。

Equifax: Consumer Fraud Division P.O.Box 740256 Atlanta, GA 30374 (888) 766-0008 www.equifax.com	Experian: Credit Fraud Center P.O.Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com	TransUnion: TransUnion LLC P.O.Box 2000 Chester, PA 19022-2000 (800) 680-7289 www.transunion.com
---	--	--

如要申请安全冻结，您将需要提供下列信息：

1. 您的全名（包括中间名缩写以及 Jr.、Sr.、II、III 等）；
2. 社会安全号码；
3. 出生日期；
4. 如果您在过去五（5）年内有搬过家，则需提供过去这五年您曾住过的地方的地址；
5. 当前地址的证明，例如一份当前的公用事业账单或电话账单；以及
6. 政府签发的身份证（州驾照或 ID 卡、军队身份证明等）的清晰影印本。

您还可联系美国联邦贸易委员会（Federal Trade Commission，“FTC”），以获得关于欺诈警报、安全冻结以及如何预防您自己不受身份盗窃影响的更多信息。FTC 的联系地址是 400 7th St. SW, Washington, D.C. 20024；电话号码 (877) 382-4357；或者 www.consumer.gov/idtheft。您可联系列于上文的信用报告机构，获得关于在您的信用报告上设置欺诈警报和/或信用冻结的信息。

5. 我可如何了解我的信息是否已经受到攻击？

在未来 45 到 60 天内，我们预期会向个人信息有受到影响、学校也有他们的当前联系详情的人发送恰当的个别通知。这些调查工作需要时间，我们也在一步步认真工作的同时，尽快做到提供准确的信息。

6. 学校是否在提供任何信用监测？

是。由于保护 UC 成员社区是应优先处理的事情，学校已及时为整个学校社区安排了通过益博睿 [IdentityWorks](#) 的免费信用监测和身份盗窃保护服务；点击 [here](#)（此处）注册。学校还通过电子邮件和在学校网站上发布通知告知了该社区。一些校园还组织了互动讲座。

7. 我要如何注册获得益博睿 IdentityWorks？

学校已经为整个学校社区安排了通过益博睿 [IdentityWorks](#) 的免费信用监测和身份盗窃保护服务；点击 [here](#)（此处）为成年人注册，点击 [here](#)（此处）为未成年人注册。

8. 我若收到益博睿发来的确认函，信中指出有在互联网上发现我的信息，我应该做什么？

如果您有收到益博睿的通知，则证明该监测服务有在发挥作用。益博睿会员门户网站提供关于您可以为保护自己做什么的信息。

益博睿建议人们根据受到攻击的信息类型采取不同的步骤。

a) 我的电子邮件地址被泄露；我接下来应该做什么？

- 考虑修改您的电子邮件的密码，以及以您的电子邮件地址作为用户名的任何其他账户的密码。使用强密码，避免在多个网站上重复使用相同密码。
- 审阅所有三家征信机构（益博睿、Equifax 和 Transunion）为您提供的信用报告，注意近期的新活动。
- 作为预防措施，留意您的银行和信用卡账户上不熟悉的交易。

b) 我的电话号码被泄露；我接下来应该做什么？

- 注意可疑来电，并且在此类来电有明显增多时联系您的电话服务提供商。
- 将您的姓名添加到全国 [Do Not Call list](#)（谢绝来电名单）。
- 审阅所有三家征信机构（益博睿、Equifax 和 Transunion）为您提供的信用报告，注意近期的新活动。
- 作为预防措施，留意您的银行和信用卡账户上不熟悉的交易。

c) 我的驾照被泄露；我接下来应该做什么？

- 联系您当地的机动车辆管理局（DMV）。
- 审阅所有三家征信机构（益博睿、Equifax 和 Transunion）为您提供的信用报告，注意近期的新活动。
- 作为预防措施，留意您的银行和信用卡账户上不熟悉的交易。

d) 我的医疗 ID 被泄露；我接下来应该做什么？

- 联系您的医疗保健提供者，以报告活动，并且查对没有任何待决定的欺诈性索赔案件。
- 审阅所有三家征信机构（益博睿、Equifax 和 Transunion）为您提供的信用报告，注意近期的新活动。
- 作为预防措施，留意您的医疗保险账户以及您的银行和信用卡账户上不熟悉的交易。

e) 我的借记卡、信用卡或零售卡信息被泄露；我接下来应该做什么？

- 审阅账户的交易历史，密切注意不熟悉的收费。
- 若您发现不熟悉的收费或其他可疑活动，则请联系您的金融机构，以取消您的卡片并/或者报告卡片被盗。
- 审阅所有三家征信机构（益博睿、Equifax 和 Transunion）为您提供的信用报告，注意近期的新活动。
- 作为预防措施，留意其他银行和信用卡账户上不熟悉的交易。

f) 我的护照信息被泄露；我接下来应该做什么？

- 联系美国护照办公室（或者在您的护照由其他国家签发时，联系您的代表大使馆或领事馆）。
- 审阅所有三家征信机构（益博睿、Equifax 和 Transunion）为您提供的信用报告，注意近期的新活动。

g) 我的银行账户信息被泄露；我接下来应该做什么？

- 审阅账户的交易历史，密切注意不熟悉的收费。
- 若您发现不熟悉的收费或其他可疑活动，则请联系您的金融机构并注销您的银行卡/账户。
- 审阅所有三家征信机构（益博睿、Equifax 和 Transunion）为您提供的信用报告，注意近期的新活动。
- 作为预防措施，留意其他银行和信用卡账户上不熟悉的交易。

h) 我的国际银行卡号（IBAN）被泄露；我接下来应该做什么？

- 审阅账户的交易历史，密切注意不熟悉的收费。
- 若您发现不熟悉的收费或其他可疑活动，则请联系您的金融机构并注销您的银行卡/账户。
- 审阅所有三家征信机构（益博睿、Equifax 和 Transunion）为您提供的信用报告，注意近期的新活动。
- 作为预防措施，留意其他银行和信用卡账户上不熟悉的交易。

i) 我的国家身份证号码被泄露；我接下来应该做什么？

- 审阅所有三家征信机构（益博睿、Equifax 和 Transunion）为您提供的信用报告，注意近期的新活动。
- 作为预防措施，留意您的银行和信用卡账户上不熟悉的交易。

j) 我在益博睿互联网监控通知（Experian Internet Surveillance）中收到一家信息被泄公司的名称。

这可能是互联网泄露来源的公司或网站。黑客在黑网上分享被盗数据时，有时会提供被泄露的信息的来源公司或网站的名称。在这次情况中，您可能会看到对 UC 的提及。

如果您不认识信息被泄的公司，不认为其是与您有过关系的公司，请注意该公司可能是同与您有过业务往来的公司有联系的第三方组织。假设的例子可能是，您曾从一家商业航空公司购买机票，而与这家公司有伙伴关系的付款处理商的数据被泄，您的信息也在此次外泄事件中受到攻击。

k) 有发现新的查询警报；我接下来应该做什么？

如果您能认出或有授权该活动，则无须采取任何行动。如果不能，则可 [here](#)（在此）了解可能有帮助的更多信息。

如果您依然确定您没有授权本活动，则可采取的步骤有：

- 联系债权人——这可能可以清楚了解具体是怎么回事。
- 审阅您的信用报告，注意近期的新活动。
- 针对您的信用报告上的账户信息提出 [Dispute](#)（异议）。

l) 有发现新账户或新交易警报；我接下来应该做什么？

如果您能认出或有授权该活动，则无须采取任何行动。如果不能，则可 [here](#)（在此）了解可能有帮助的更多信息。

若您依然确定您没有授权本活动，也有可采取的步骤。

- 联系债权人——这可能可以清楚了解具体是怎么回事。
- 审阅您的信用报告，注意近期的新活动。
- 针对您的信用报告上的账户信息提出 [Dispute](#)（异议）。

m) 我不认识我的信用警报中的公司。

如果您不确定自己是否有发起您的警报上的活动，下面是一些可能有帮助的信息：

您最近是否有提交信用申请或新开账户？有些公司，您可能在警报上第一眼看到时感觉不熟悉，例如：

- JPMCB（又名 JP Morgan Chase Bank）
- CBNA（又名 Citibank）
- CapOne（又名 CapitalOne）
- FNBO（又名 First National Bank of Omaha）
- TBH（又名 The Home Depot）
- Synchrony Bank——通常与主要零售商合作的借款和贷款提供商。
- Credco——这是一家第三方报告机构。抵押贷款公司、金融机构和经销商经常会联系此类报告机构，以获得一个三家机构信用评分。

- **Ally**——Ally Bank 是一家借款和贷款提供商，通常在多个行业与主要零售商合作，例如汽车融资、股权发起人和公司理财。

n) 我申请了借款，但没有收到警报

大多数贷款方在 30 天内报告账户活动，但有些会花上长达 90 天。另外，有些较小的债权人可能仅向三大全国消费者报告机构——Equifax、益博睿和 TransUnion 中的一家或两家报告。如果您的债权人没有三家全报，您则不会针对同一活动收到来自所有三家的警报。

o) 我为什么有针对同一贷款申请收到不止一个警报？

您将针对同一贷款申请收到多个警报的一些常见原因有：

- 如果该贷款获批，贷款方也开设了一个您名下的账户，您则将收到针对为处理申请做出的初次信用报告查询的警报，还会因开户收到警报。
- 如果贷款方有向全部三大征信机构——益博睿、Equifax 和 TransUnion 报告您的账户，您则可能从各家机构收到一个警报。

p) 我的 SSN 被泄露；我接下来应该做什么？

您可拨打益博睿的联系电话 (888) 397 3742。我们要求学校社区的成员做到一直对身份盗窃或欺诈等威胁保持警惕。除此之外，对“网络钓鱼”电子邮件，或者来电人表现出一副他们认识您的样子或声称是您可能有业务往来的公司的电话，以及让您提供敏感信息（例如密码、社会安全号码、财务账户信息等）的要求等提高警惕，总是一个好主意。您可将疑似网络钓鱼或试图实施社交工程诈骗的报告发送至 communications@ucop.edu。我们还建议您为有提供多因素验证的在线账户设置此类验证流程。

关于获得免费的信用报告的信息

依照美国法律，美国居民有每年从三大征信机构中的各家获得一份免费信用报告的权利。如要获得您的免费信用报告，可访问 www.annualcreditreport.com 或拨打免费电话 (877) 726-1014。

关于执行欺诈警报或安全冻结的信息

您可使用下文给出的地址联系三大征信机构，以在您的信用报告上设置欺诈警报。欺诈警报会向任何请求获得您的信用档案的人显示您怀疑自己可能是欺诈的受害者。欺诈警报不会影响您获得贷款或借款的能力。该警报只是会警示企业您的个人信息可能已被泄露，需要该企业在为您发放借款前核实您的身份。如果您是借款的申请人，这可能会导致一些短期延迟，但这么做可能会保护您，以防他人使用您的姓名获得借款。

除了欺诈警报外，您还可考虑在您的信用报告上设置安全冻结。安全冻结会禁止信用报告机构在没有书面授权的情况下透露消费者信用报告中的任何信息。还请您注意，在您的信用报告上设置安全冻结，可导致您为获得新的贷款、借款、抵押贷款、就业、住房或其他服务提交的申请的及时获批有延迟、被干扰或阻止。信用报告机构可能不会针对设置、暂时取消或永久撤销安全冻结向您收取费用。

如要在您的信用报告上设置欺诈警报，您必须联系下列三家征信机构中的一家，其余两家会自动添加欺诈警报。如要在您的信用报告上设置安全冻结，您必须联系下列三家征信机构中的一家。

Equifax: Consumer Fraud Division P.O.Box 740256 Atlanta, GA 30374 (888) 766-0008 www.equifax.com	Experian: Credit Fraud Center P.O.Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com	TransUnion: TransUnion LLC P.O.Box 2000 Chester, PA 19022-2000 (800) 680-7289 www.transunion.com
---	--	--

如要申请安全冻结，您将需要提供下列信息：

1. 您的全名（包括中间名缩写以及 Jr.、Sr.、II、III 等）；
2. 社会安全号码；
3. 出生日期；
4. 如果您在过去五（5）年内有搬过家，则需提供过去这五年您曾住过的地方的地址；
5. 当前地址的证明，例如一份当前的公用事业账单或电话账单；以及
6. 政府签发的身份证（州驾照或 ID 卡、军队身份证明等）的清晰影印本。

您还可联系美国联邦贸易委员会（Federal Trade Commission，“FTC”），以获得关于欺诈警报、安全冻结以及如何预防您自己不受身份盗窃影响的更多信息。FTC 的联系地址是 400 7th St. SW, Washington, D.C. 20024；电话号码 (877) 382-4357；或者 www.consumer.gov/idtheft。您可联系列于上文的信用报告机构，获得关于在您的信用报告上设置欺诈警报和/或信用冻结的信息。

9. 我若不是有证件的居民，是否可以获得信用监测？

要获得信用服务，您必须是年满 18 岁，有在美国建立信用记录，有在您名下的社会安全号码，并且有与您的信用档案相关的美国居住地址。

10. 除了与益博睿合作采取直接行动以外，我是否应该告知学校任何我的数据受影响的情况

没有必要告知学校因 Accellion 事件受影响的数据。学校目前正在努力确定哪些社区成员的个人信息受到影响，以及他们的联系信息。这些调查工作需要时间，我们也在一步步认真工作的同时，尽快做到提供准确的信息。在未来 45~60 天内，我们预期会获得我们需要的信息，以向学校有他们的当前联系详情的人发送个别通知。

11. 我是否可以查看我的信用报告？

是。信用监测机构的建议是，您应该至少每年查看您的信用报告一次（如果无法更频繁），作为您的常规财务管理做法的一部分。有些人倾向于每月甚至每周查看一次他们的信用评分。您可以在不影响您的评分的情况下按照您的意愿随时查看您的信用评分。

12. 我是否需要为信用报告付款？

您可以每年从所有三家征信机构免费获得一次您的信用报告。您可以访问 www.annualcreditreport.com 在线完成或拨打电话 1-877-322-8228。

13. 在应对此次事件中，为了使学校网络更安全，您目前在采取哪些行动？

我们在发现问题后，有使 Accellion FTA 离线，并且修补了该弱点。没有证据显示其他学校系统有受到影响。我们正在进行的工作有：向有更强安全控制的新的文件传输系统过渡，在我们的网络内广泛部署其他系统监测，并且进行某些系统的安全健康检查；我们还在改善安全控制、程序和流程。

14. 该事件是否已经得到解决？

是。我们在发现问题后，有使该系统离线，并且修补了 Accellion 弱点。没有证据显示其他学校系统有受到影响。我们正在进行的工作有：向有更强安全控制的新的文件传输系统过渡，在我们的网络内广泛部署其他系统监测，并且进行某些系统的安全健康检查；我们还在改善安全控制、程序和流程。

15. 您是否有通知相应的权威机构？

是。学校已将该事宜报告到美国联邦执法机关。

16. 多因素验证是什么？

验证是决定某人或某事是否确实是其声称自己是的人或事的程序。多因素验证（MFA）是一个要求使用超过一种来自分别独立的认证机制的验证方法，以为登录或其他交易验证用户的身份的安全系统。多因素验证结合两种或两种以上独立的认证机制：用户知道什么（密码）、用户拥有什么（安全令牌）以及用户是什么（生物特征识别核对）。

17. 我若有其他问题应该怎么办？

可将关于本事件的问题发至 communications@ucop.edu。