内容

关于发生了什么以及我们正在做什么的常见问题

1. 发生了什么？

2020年12月24日，学校的 Accellion 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。学校于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，并且正在：

- 向更加安全的解决方案过渡；
- 配合 FBI；以及
- 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。

5月12日至14日期间，学校有向信息可能受到影响的 UC 社区成员发送电子邮件。由于透明度原因，并且出于高度谨慎考虑，学校有继续在开展调查期间向信息可能受到影响的社区成员发出通知。

截至2021年6月30日和7月1日，学校已经确定信息有受到 Accellion 事件影响的个别社区成员，并且已通过益博睿发出恰当的个别通知。UC 社区成员会在有其当前物理地址时收到通过 USPS 信函发出的通知。学校若没有物理地址，但有电子邮件地址，则将通过电子邮件发出该通知。学校有在一步步认真工作的同时，尽快做到提供准确的信息。

2. Accellion 事件有影响哪些人的信息？

从 Accellion 调查获得的证据显示，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（现任和前任）和他们的受抚养人、退休人员和受益人，以及目前是学校学生和参与过 UC 计划的其他个人。截至2021年6月30日和7月1日，学校已经确定信息有受到 Accellion 事件影响的个别社区成员，并且已通过益博睿发出恰当的个别通知。

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，以及提供给 UC 的其他个人信息。曾参与2020年加利福尼亚大学本科生体验问卷调查（UCUES）的学生提供的信息也有受到影响，有被威胁行事人发布到互联网上。

通过彻底调查，截至2021年6月30日和7月1日，学校已经确定信息有受到 Accellion 事件影响的个别社区成员，并且已通过益博睿发出恰当的个别通知。UC 社区成员会在有其当前物理地址时收到通过 USPS 信函发出的通知。学校若没有物理地址，但有电子邮件地址，则将通过电子邮件发出该通知。学校有在一步步认真工作的同时，尽快做到提供准确的信息。

4. 这件事情为什么有花这么长时间？

学校已经知道发布在互联网上的数据。即便如此，为了对受此次攻击影响的整个范围有一个全面完整的了解，已经聘请了一家行业领先的司法网络安全公司，以决定具体发生了什么，未经授权被访问或获得的数据有哪些。

作为该调查工作的一部分，并且为了向学校社区成员提供准确的信息，学校已经开始与 UCOP 安全团队和我们的外部网络安全专家合作，重现在相关时间段内可能存储在 Accellion FTA 的文件有哪些。作为这项工作的一部分，学校已经启动了开展认真检查各份和每份文件工作的过程，以决定可能受影响的信息有哪些，从而能够为各位个人信息受影响的学校社区成员提供准确的信息并发出通知。

除了借助尖端的数据解析和搜索工具以外，学校还有进行人工审阅各份和每份文件的工作。由于这些数据中的很多数据是无结构化的，再加上文件数目很庞大，该过程是一项耗时耗力的工作，需要数百小时的详细审阅和分析。学校有利用其资源，以尽快完成此次调查和分析；截至2021年6月30日和7月1日，学校已经通过益博睿发出恰当的个别通知。

在调查工作还在进行中时，学校在其网站上更新了关于该事件的信息，并且有向信息可能受到影响的个人群体发送电子邮件，在邮件中提供了如何采取措施保护他们自己的指南，并有附上益博睿 IdentityWorks 提供的免费信用监测和身份盗窃保护服务。

5. 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？

学校在发现该问题后，有使 Accellion FTA 离线，并且修补了程序弱点。没有证据显示其他学校系统有受到影响。学校正在进行的工作有：向有更强安全控制的新的文件传输系统过渡，在学校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；还在改善安全控制、程序和流程。

6. 该事件是否已经得到解决？

是。学校在发现该问题后，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。学校正在进行的工作有：向有更强安全控制的新的文件传输系统过渡，在学校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；还在改善安全控制、程序和流程。

7. 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。

关于您可以做什么的常见问题

8. 我需要做什么吗？

学校请学校的社区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下列电子邮件地址（根据您的校区）：

- UC Berkeley - phishing@berkeley.edu
- UC Davis & UC Davis Health - cybersecurity@ucdavis.edu
- UC Irvine & UC Irvine Health - spam@uci.edu
- UCLA - security@ucla.edu
- UCLA Health - DangerousEmail@mednet.ucla.edu
- UC Merced - infosecurity@ucmerced.edu
- UC Riverside - abuse@ucr.edu
- UC San Diego & UCSD Health - abuse@ucsd.edu
- UC San Francisco & UC San Francisco Health – ITServiceDesk@ucsf.edu
- UC Santa Barbara - security@ucsb.edu
- UC Santa Cruz – help@ucsc.edu

学校还建议您轮换密码，并且为有提供多因素验证的在线账户设置此类验证流程。

学校目前通过益博睿 IdentityWorks 为下列群体提供免费的信用监测和身份盗窃保护服务：

- 员工（现任和前任）和他们的受抚养人；
- 退休人员和受益人；
- 目前是学校学生；以及
- 曾参与学校计划的某些其他个人

这些个人已经在2021年5月12日～14日间收到通知。该电子邮件中包含了一个激活代码。将再也无法使用之前的通用激活代码（JCZGTC333）进行新的激活。

通过彻底调查，截至2021年6月30日和7月1日，学校已经确定信息有受到 Accellion 事件影响的个别社区成员，并且已通过益博睿发出恰当的个别通知。UC 社区成员会在有其当前物理地址时收到通过 USPS 信函发出的通知。学校若没有物理地址，但有电子邮件地址，则将通过电子邮件发出该通知。学校有在一步步认真工作的同时，尽快做到提供准确的信息。

9. 我可如何了解我的信息是否已经受到攻击？

学校目前正在努力确定信息受到影响的社区成员。这些调查工作需要时间，学校也在一步步认真工作，以尽快提供准确的信息。截至2021年6月30日和7月1日，学校已经通过益博睿发出恰当的个别通知。UC 社区成员会在有其当前物理地址时收到通过 USPS 信函发出的通知。学校若没有物理地址，但有

电子邮件地址，则将通过电子邮件发出该通知。这些通知还有包含益博睿 IdentityWorks 的信用监测和身份盗窃保护激活代码。

10. 我的 SSN 被泄露。我接下来应该做什么？

学校社区成员应该做到一直对身份盗窃或欺诈等威胁保持警惕。您可通过定期查看并监测您的账户账单和信用记录，注意任何未经授权的交易或活动的迹象。您若怀疑自己是身份盗窃或欺诈的受害者，可联系您当地的警察局。您也可联系信用报告机构，以在您的信用报告上设置“欺诈警报”或“安全冻结”，以防身份欺诈或盗窃。

11. 我相信我是身份欺诈或盗窃的受害者。我接下来应该做什么？

学校社区成员应该做到一直对身份盗窃或欺诈等威胁保持警惕。您可通过定期查看并监测您的账户账单和信用记录，注意任何未经授权的交易或活动的迹象。您若怀疑自己是身份盗窃或欺诈的受害者，可联系您当地的警察局。

您可联系信用报告机构，以在您的信用报告上设置“欺诈警报”或“安全冻结”。

- 提交警察报告，并且要求获得一份您的报告的副本。
- 向联邦贸易委员会提交投诉。
- 向您所在州的总检察长提交投诉。
- 保留详细的记录。
- 保留详细的记录，记下您针对本事件都与谁交谈过，他/她有告诉您什么内容，以及该对话的日期。
- 保留所有与可疑或欺诈性活动、身份盗窃或欺诈相关的书信往来和表格的原始版本。
- 保留支持性文件的原始版本，例如警察报告以及与债权人的来往书信。当需要按要求提供支持性文件时，发送副本。
- 保留以前的文件，即使您相信相关问题已经得到解决。

您还可联系附属金融机构，以保护或注销任何已经被篡改或属于欺诈开设的账户。

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下列电子邮件地址（根据您的校区）：

- UC Berkeley - phishing@berkeley.edu
- UC Davis & UC Davis Health - cybersecurity@ucdavis.edu
- UC Irvine & UC Irvine Health - spam@uci.edu
- UCLA - security@ucla.edu
- UCLA Health - DangerousEmail@mednet.ucla.edu
- UC Merced - infosecurity@ucmerced.edu
- UC Riverside - abuse@ucr.edu
- UC San Diego & UCSD Health - abuse@ucsd.edu
- UC San Francisco & UC San Francisco Health – ITServiceDesk@ucsf.edu
- UC Santa Barbara - security@ucsb.edu
- UC Santa Cruz – help@ucsc.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) 322-8228。在2022年4月20日前，益博睿、TransUnion 和 Equifax 将通过 AnnualCreditReport.com 为所有美国消费者提供免费的每周信用报告，以帮助您在 COVID-19 导致的前所未有的突发困难时期保护您的财务健康。

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金融信用的能力。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金融信用前核实您的身份。如果您是金融信用的申请人，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金融信用。

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、金融信用、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，您必须联系所有下列三家征信机构。

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、安全冻结以及如何确保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。

12. 我是否应该报告可疑或实际的身份盗窃或欺诈事件？

如果您怀疑或知道自己已经成为身份盗窃或欺诈的受害者，我们敦促您向执法机构、联邦贸易委员会和您所在州的总检察长报告该事件。

关于信用监测的问题

13. 学校是否在提供任何信用监测？

学校目前通过益博睿 IdentityWorks 为下列群体提供免费的信用监测和身份盗窃保护服务：

- 员工（现任和前任）和他们的受抚养人；
- 退休人员和受益人；

- 目前是学校学生；以及
- 曾参与学校计划的某些其他个人

这些个人已经在2021年5月12日～14日间收到通知。该电子邮件中包含一个注册获得益博睿 IdentityWorks 的激活代码。将再也无法使用之前的通用激活代码（JCZGTC333）进行新的激活。

截至2021年6月30日和7月1日，学校已经通过益博睿发出恰当的个别通知。UC 社区成员会在有其当前物理地址时收到通过 USPS 信函发出的通知。学校若没有物理地址，但有电子邮件地址，则将通过电子邮件发出该通知。这些通知还有包含益博睿 IdentityWorks 的信用监测和身份盗窃保护激活代码。

14. 我是否有资格获得免费的信用监测？

有资格获得免费的信用监测的个人有：

- 员工（现任和前任）和他们的受抚养人；
- 退休人员和受益人；
- 目前是学校学生；以及
- UC 外展计划的参与人。

如果您属于这些类型之一，但没有收到个别代码，请拨打我们专门的接线中心 1-866-904-6220 获得援助。

15. 如果我在我的信用档案上设置欺诈警报，会发生什么？

您有权免费在您的档案上设置初期或延期“欺诈警报”。初期欺诈警报为期一年，可在消费者的信用档案上设置该警报。企业在看到消费者的信用档案上有显示欺诈警报时，必须在提供新的金融信用前采取核实消费者的身份的步骤。您若是身份盗窃的受害者，则有权获得延期欺诈警报，该欺诈警报为期七年。您可联系全国三大征信机构中的任一家——Equifax、益博睿和 TransUnion，以申请获得欺诈警报。一旦您同其中的一家征信机构设置警报，这家机构会将您的请求发给其余两家。

16. 如果我在我的信用档案上设置冻结，会发生什么？

安全冻结将禁止消费者报告机构在没有您的明确授权的情况下透露您的信用报告中的信息。安全冻结旨在防止金融信用、贷款和服务未经您同意在您的名下获批。

不过您也应该注意，使用安全冻结从可获得您的信用报告上的个人和财务信息的人手中拿回控制权，可能会延迟、干扰或阻止任何您在之后为获得新的贷款、金融信用、抵押贷款或任何其他涉及金融信用延期提出的请求或申请的及时批准。

依照联邦法律，不可针对设置或取消您的信用报告上的安全冻结向您收取费用。直接联系三大征信机构，以在您的信用档案上设置安全冻结。

17. 设置欺诈警报具体是指什么？

可以免费在您的信用报告上设置欺诈警报，具体类型有两种：

- **初期（一年）欺诈警报**可以被设置，如果您相信您是或者可能成为欺诈或身份盗窃的受害者。该欺诈警报为期一年。如果您希望您的信用报告上依然有该设置，您将需要在该期限后为警报续期。当您或他人试图在您的名下开户，或者试图修改现有账户（例如增加信用额度）时，贷款方或债权人必须在完成申请处理前，采取合理的步骤，以确定您确实是自称之人，例如通过拨打您提供的电话号码联系您。

设置初期欺诈警报还可使您除了获得依照 Fair Credit Reporting Act(《公平信用报告法》）有权从各家征信机构获得的一份免费报告外，还能够每隔12个月申请从全国三大征信机构获得一份免费的信用报告。

- **延期欺诈警报**可以被设置，如果您是欺诈或身份盗窃的受害者。该设置要求提供一份有效的警察或执法机构的报告或 Federal Trade Commission Identity Theft Report（联邦贸易委员会身份盗窃报告）的副本。延期欺诈警报与初期欺诈警报相似，但可持续七年。在有延期欺诈警报设置时，贷款方或债权人必须按要求面对面，或者拨打您在开立新账户或修改现有账户前提供的电话号码，核实您的身份。

18. 我若不是有证件的居民 / 美国公民，是否可以获得信用监测？

必须有社会安全号码才可注册获得信用监测。没有社会安全号码的成年人有资格获得益博睿 IdentityWorks 全球版。您可拨打益博睿的联系电话 1-866-904-6220；代表学校工作的益博睿代表将协助您。

19. 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。

20. 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 1-866-322-8228。一般情况下，您可在 AnnualCreditReport.com 每隔12个月从各家机构获得一份免费的信用报告。但在2022年4月底前，您可每周要求获得一份免费的信用报告。

关于益博睿的问题

21. 我要如何注册获得益博睿 IdentityWorks？

有资格享用信用监测和身份盗窃保护服务的个人已经在2021年5月12日～14日间收到通知。该电子邮件中包含一个注册获得益博睿 IdentityWorks 的激活代码。将再也无法使用之前的通用激活代码（JCZGTC333）进行新的激活。

截至2021年6月30日和7月1日，学校已经通过益博睿发出恰当的个别通知。UC 社区成员会在有其当前物理地址时收到通过 USPS 信函发出的通知。学校若没有物理地址，但有电子邮件地址，则将通过电子邮件发出该通知。这些通知还有包含益博睿 IdentityWorks 的信用监测和身份盗窃保护激活代码。

如果您已经使用之前的通用激活代码注册获得益博睿 IdentityWorks，则无需再次注册。

22. 我已经通过益博睿注册了免费的信用监测，但也有收到个别代码。我是否需要为确保我的信用被监测做任何事情？

不需要。如果您已经使用之前的代码注册了免费的信用监测，则不必采取其他步骤。

23. 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？

如果您之前注册了益博睿 IdentityWorks 并有收到警报，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。
- 您若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。
- 您若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。
- 您若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。

这是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。

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）。

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金融信用和贷款提供商。
- 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 是一家金融信用和贷款提供商，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) 我申请了金融信用，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：

- 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，您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。

24. 我的代码不再有效，或者我有收到错误信息。我要怎么办呢？

在2021年5月12日～14日间，有资格的社区成员已经被发送一封包含一个特殊的激活代码的电子邮件。将再也无法使用之前的通用激活代码（JCZGTC333）进行新的激活。

截至2021年6月30日和7月1日，学校已经通过益博睿发出恰当的个别通知。UC 社区成员会在有其当前物理地址时收到通过 USPS 信函发出的通知。学校若没有物理地址，但有电子邮件地址，则将通过电子邮件发出该通知。这些通知还有包含益博睿 IdentityWorks 的信用监测和身份盗窃保护激活代码。

如果您已经使用之前的通用激活代码注册获得益博睿 IdentityWorks，则无需再次注册。

25. 益博睿要求我为获得信用监测分享我的 SSN。益博睿目前有使用什么样的安全协议？

Experian®（益博睿）是美国三大征信机构中的一家。参阅 Experian's approach to privacy（益博睿的隐私措施）。

26. 我没有收到个别代码。我应该做些什么？

有资格享用信用监测和身份盗窃保护服务的个人已经在2021年5月12日～14日间收到通知。截至2021年6月30日和7月1日，学校已经通过益博睿发出恰当的个别通知。这些通知还有包含益博睿 IdentityWorks 的信用监测和身份盗窃保护激活代码。

该信函或电子邮件中包含一个注册获得益博睿 IdentityWorks 的激活代码。

有资格获得免费的信用监测的个人有：

- 员工（现任和前任）和他们的受抚养人；
- 退休人员和受益人；
- 目前是学校学生；以及
- UC 外展计划的参与人。

27. 我还没有收到通知，但我相信自己有资格享用信用监测。

请检查您的电子邮件，查看是否有收到益博睿在2021年6月30日到7月1日之间发出的邮件。还请查看您的垃圾邮件文件夹。

截至2021年6月30日和7月1日，学校已经通过益博睿发出恰当的个别通知。UC 社区成员会在有其当前物理地址时收到通过 USPS 信函发出的通知。学校若没有物理地址，但有电子邮件地址，则将通过电子邮件发出该通知。这些通知还有包含信用监测，激活代码也被包含在该信函或电子邮件中，以注册获得益博睿。

有资格获得免费的信用监测的个人有：

- 员工（现任和前任）和他们的受抚养人；

- 退休人员和受益人；
- 目前是学校学生；以及
- UC 外展计划的参与人。

如果您属于这些类型之一，但没有收到个别代码，请拨打我们专门的接线中心 1-866-904-6220 获得援助。

28. 我相信自己是有资格通过益博睿 IdentityWorks 获得信用监测和身份盗窃保护的人，但我无法完成信用监测的验证过程，原因是我：

- **没有信用档案；**
- **不住在美利坚合众国；**
- **或者没有社会安全号码。**

对我可用的服务有哪些？

信用档案（通常被称作信用记录）、美国地址和社会安全号码是获得信用监测的必要因素。没有信用记录的个人可注册加入益博睿的 Identity Product（身份产品），该服务包括互联网监控、一百万美元身份盗窃保险和全方位服务身份恢复。

如果您有资格，则可使用激活代码注册获得益博睿的 Identity Product（身份产品），可在2021年5月12日到5月14日之间发给您的个别通知中找到该激活代码。截至2021年6月30日和7月1日，学校已经通过益博睿发出恰当的个别通知。UC 社区成员会在有其当前物理地址时收到通过 USPS 信函发出的通知。学校若没有物理地址，但有电子邮件地址，则将通过电子邮件发出该通知。这些通知还有包含益博睿 IdentityWorks 的信用监测和身份盗窃保护激活代码。

益博睿代表会积极回答您可能有的任何问题；可拨打1-866-904-6220联系他们。

29. 如果我的益博睿注册因为我是未成年人或者没有信用档案而验证失败，我应该做什么？

信用档案通常被称作信用记录，是获得信用监测的必要因素。没有信用记录的个人可注册加入益博睿的 Identity Product（身份产品），该服务包括互联网监控、一百万美元身份盗窃保险和全方位服务身份恢复。

如果您有资格，则可使用激活代码注册获得益博睿的 Identity Product（身份产品），可在2021年5月12日到5月14日之间发给您的个别通知中找到该激活代码。截至2021年6月30日和7月1日，学校已经通过益博睿发出恰当的个别通知。UC 社区成员会在有其当前物理地址时收到通过 USPS 信函发出的通知。学校若没有物理地址，但有电子邮件地址，则将通过电子邮件发出该通知。这些通知还有包含益博睿 IdentityWorks 的信用监测和身份盗窃保护激活代码。

益博睿代表会积极回答您可能有的任何问题；可拨打1-866-904-6220联系他们。

30. 多因素验证是什么？

验证是决定某人或某事是否确实是他们声称是的人或事的程序。多因素验证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（生物特征识别查对）。

其他/学校支持和资源

31. 我是否应该告知学校我的任何数据有受影响？

没有必要告知学校因 Accellion 事件受影响的数据。

32. 我是否应该更改我的密码？

目前没有证据显示登录凭证被泄露。无论如何，定期更改您的密码都是最佳做法。

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下列电子邮件地址（根据您的校区）：

- UC Berkeley - phishing@berkeley.edu
- UC Davis & UC Davis Health - cybersecurity@ucdavis.edu
- UC Irvine & UC Irvine Health - spam@uci.edu
- UCLA - security@ucla.edu
- UCLA Health - DangerousEmail@mednet.ucla.edu
- UC Merced - infosecurity@ucmerced.edu
- UC Riverside - abuse@ucr.edu
- UC San Diego & UCSD Health - abuse@ucsd.edu
- UC San Francisco & UC San Francisco Health – ITServiceDesk@ucsf.edu
- UC Santa Barbara - security@ucsb.edu
- UC Santa Cruz – help@ucsc.edu

我们还建议您轮换密码，并且为有提供多因素验证的在线账户设置此类验证流程。

33. 我的学生 ID 是否有受影响？

某些学生 ID 有受影响。截至2021年6月30日和7月1日，学校已经通过益博睿发出恰当的个别通知。本通知包含关于受影响数据的信息。

UC 社区成员会在有其当前物理地址时收到通过 USPS 信函发出的通知。学校若没有物理地址，但有电子邮件地址，则将通过电子邮件发出该通知。这些通知还有包含益博睿 IdentityWorks 的信用监测和身份盗窃保护激活代码。

34. 我如果担心自己的身体、心理或情绪健康，学校有哪些资源？

学校社区内有很多心理和情绪健康支持以及安全计划资源供大家使用：

- **咨询和心理服务**——学生可通过校园内相应的咨询和心理服务办公室（有时被称作 CAPS），获得保密的心理和情绪健康支持：
  - Berkeley
  - Davis
  - Irvine
  - Los Angeles
  - Merced
  - Office of the President
  - Riverside
  - San Diego
  - San Francisco
  - Santa Barbara
  - Santa Cruz

- **教职人员和工作人员援助计划**——学校内的各个校区、医疗中心和国家实验室负责管理其各自的教职人员和工作人员援助计划（有时被称作 Employee Assistance Program - 员工援助计划）。援助

计划提供免费保密的情绪健康资源，有时可直接在校园内轻松获得短期咨询、评估和转介服务。如需了解在具体 UC 地点可以使用的援助计划的详情，点击 here（此处）。

- **CARE**——若是性暴力、亲密伴侣暴力或跟踪的幸存者，请联系 UC CARE 支持者，以获得怀着同情心提供的保密支持和安全计划。如需了解您所在校区的 CARE 办公室的详情，点击 here（此处）。如果您的处境危险或者立即需要帮助，拨打9-1-1。

如果您需要的支持超出 UC 社区范围，这些办公室也可提供关于可能可用的当地资源的信息。

35. 目前有为社区的国际成员提供哪些特殊照顾？

必须有社会安全号码才可注册获得信用监测。没有社会安全号码的成年人有资格获得益博睿 IdentityWorks 全球版。2021年5月12日～5月14日以及6月30日～7月1日之间发出的个别通知中有一个激活代码，也可使用该代码注册益博睿 IdentityWorks 全球版。

36. 我若有其他问题应该怎么办？

学校有安排通过益博睿的专门接线中心。您若有关于该事件或学校的回应的任何问题，益博睿代表会积极回答这些问题。可拨打 1-866-904-6220 联系这些代表。

37. 我希望针对发生了什么直接与 UC 交谈。

可将关于本事件的问题发至 communications@ucop.edu。

关于 UCUES 的问题

1. **UCUES 是什么？**
   The University of California Undergraduate Experience Survey（加利福尼亚大学本科生体验问卷调查，UCUES）征求学生对学术和共同课程等广泛体验的意见，包括教学、指导和学生服务。UCUES 提供关于学生看法和行为的信息，包括时间利用、学术参与和社区参与。该调查评估学生对校园生活的多个不同方面的看法，包括学术指导、校园环境、课程和教学以及与教职人员的互动。它会记录学生的自我认知和目标、政治信仰，以及学生对该研究型大学起到的作用的看法。该调查收集人口统计背景信息，例如第一语言、家庭移民背景和社会阶层。

2. **UC 为什么进行 UCUES？**
   UCUES 一直以来有被广泛利用，以引导学校提升本科生体验。校区也会利用 UCUES 来向他们的学术参议员报告他们的学术计划的质量。有些校区曾在他们的 WASC 认可自我研究中用到 UCUES 数据。还有些校区，以及学生事务副校长理事会，借助 UCUES 来评价他们的学生服务的质量和使用情况。多所校区曾利用 UCUES，做出针对校园环境和多元化对学生教育经历的影响的报告。
   UCUES 数据和结果曾在 UC 的年度问责报告、UC 当前运营预算中被使用，还曾被用来告知校务委员会的成员，例如长远指导小组（Long-Range Guidance Team）、多元化研究团队（Diversity Study Group）和学生基础需求委员会（Student Basic Needs Committee）。

3. **其他问卷调查是否有受到 Accellion FTA 安全事件的影响？**
   我们尚未发现任何其他受影响的问卷调查。

4. **UCUES 问卷调查中的哪些类型的信息有被发布到互联网上？**
   受影响的信息包括，参与者在调查中给出的全部回答，这可能包括您的姓名；电子邮件地址；学生 ID；背景和个人特征；学术参与；教育经历；个人发展和心理健康；多元化和包容性的校园环境；性行为不端情况；学生生活；以及食物和住房保障（如果您有在回答该问卷调查时提供这些信息）。可在 here（此处）获取该问卷问题的示例清单。

5. **这件事情是如何发生的？**
   学校曾使用 Accellion FTA 来传输问卷调查结果等大文件。 不幸的是，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。学校在发现该问题后，有使该系统离线，并且修补了 Accellion 弱点。我们正在进行向更加安全的解决方案的过渡。学校曾与 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。

   学校在发现该问题后，有使 Accellion FTA 离线，并且修补了程序弱点。没有证据显示其他学校系统有受到影响。学校正在进行的工作有：向有更强安全控制的新的文件传输系统过渡，在学校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；还在改善安全控制、程序和流程。

6. **学校接下来打算如何保护这些完成 UCUES 者的保密性？**
学校在发现在2020年加利福尼亚大学本科生体验问卷调查（UCUES）中收集的学生回答不幸在发生网络攻击时是 Accellion FTA 中的部分数据并被发布到互联网上时，学校便开始审阅与该两年一次的调查相关的政策和流程，以更好地保护 UC 社区的个人数据和隐私。加强这些政策和流程的过程目前在进行中。

7. **我如果担心自己的身体、心理或情绪健康，学校有哪些资源？**
学校社区内有很多心理和情绪健康支持以及安全资源供大家使用：

- **咨询和心理服务**——学生可通过校园内相应的咨询和心理服务办公室（有时被称作 CAPS），获得保密的心理和情绪健康支持：
  - Berkeley
  - Davis
  - Irvine
  - Los Angeles
  - Merced
  - Office of the President
  - Riverside
  - San Diego
  - San Francisco
  - Santa Barbara
  - Santa Cruz

- **教职人员和工作人员援助计划**——学校内的各个校区、医疗中心和国家实验室负责管理其各自的教职人员和工作人员援助计划（有时被称作 Employee Assistance Program - 员工援助计划）。援助计划提供免费保密的情绪健康资源，有时可直接在校园内轻松获得短期咨询、评估和转介服务。如需了解在具体 UC 地点可以使用的援助计划的详情，点击 here（此处）。

- **CARE**——若是性暴力、亲密伴侣暴力或跟踪的幸存者，请联系 UC CARE 支持者，以获得怀着同情心提供的保密支持和安全计划。如需了解您所在校区的 CARE 办公室的详情，点击 here（此处）。如果您的处境危险或者立即需要帮助，拨打9-1-1。

如果您需要的支持超出 UC 社区范围，这些办公室也可提供关于可能可用的当地资源的信息。

关于申请信息的问题

1. **我是申请进入某一加利福尼亚大学校区的2021-2022申请人。我的信息是否有受影响？**
已经开始或完成了加利福尼亚大学2021-2022学年申请过程的个人的联系信息有受影响。该联系信息仅限于姓名、电子邮件地址和电话号码。

   学校将单独通知这些个人，他们的通知也将包含他们可采取哪些预防措施的信息。

2. **我是申请进入某一加利福尼亚大学校区的2020-2021申请人。我的信息是否有受影响？**
已提交的加利福尼亚大学2020-2021学年申请中的信息有受影响。此类信息可能包括出生日期、性别认同、家庭全家收入水平、民族和/或部落隶属关系，还可能包括第一语言、性取向、学术信息（GPA、测试分数）以及您是否曾接受寄养照顾。

   学校会单独通知这些个人，他们的通知还包含他们可采取哪些预防措施的信息。

3. 我是2020-2021、2021-2022学年加利福尼亚大学（UC）系统的申请人。对我可用的资源有哪些？

学校将单独通知2020-2021、2021-2022学生申请人。他们的通知会包含他们可采取哪些预防措施的信息。

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 或下列电子邮件地址（根据您的校区）：

- UC Berkeley - phishing@berkeley.edu
- UC Davis & UC Davis Health - cybersecurity@ucdavis.edu
- UC Irvine & UC Irvine Health - spam@uci.edu
- UCLA - security@ucla.edu
- UCLA Health - DangerousEmail@mednet.ucla.edu
- UC Merced - infosecurity@ucmerced.edu
- UC Riverside - abuse@ucr.edu
- UC San Diego & UCSD Health - abuse@ucsd.edu
- UC San Francisco & UC San Francisco Health – ITServiceDesk@ucsf.edu
- UC Santa Barbara - security@ucsb.edu
- UC Santa Cruz – help@ucsc.edu

我们还建议您轮换密码，并且为有提供多因素验证的在线账户设置此类验证流程。

关于6月30日和7月1日发出的个别通知的问题

38. 我没有在六月底 / 七月初收到学校发出的信函。这是否意味着我的数据没有受到影响？
已经在有当前联系信息时将通知发给个人信息在该事件中以及某些其他恰当的情况下受到影响的个人。

出于高度谨慎考虑，学校已于四月份和五月份，在完成了受影响数据分析工作之前，通知了个人信息*可能*受到影响的社区成员。学校还为这些个人提供了一年免费信用监测和身份盗窃保护。

39. 有在什么时候发出个别通知？
这些通知于6月30日和7月1日发出。

40. 是否应该期待收到电子邮件或通过 USPS 邮寄的信函？
UC 社区成员会在我们有其当前物理地址时收到通过 USPS 信函发出的通知。学校若没有物理地址，但有电子邮件地址，则会通过电子邮件发出该通知。

41. 如果个别通知是通过电子邮件发出，那么发出通知的电子邮件地址是什么？
USPS 信函和/或电子邮件已于6月30日和7月1日之间由益博睿发出。发出通知的益博睿电子邮件地址是“no-reply@marketing.csid.com”，并且有说明加利福尼亚大学是发件人。

42. 我的哪些数据有在 Accellion 事件中受到影响？
有在您的通知信函中说明受影响的个人信息。

43. 我没有在学校于六月份发给我的个别通知信函或电子邮件中收到激活代码。我应该做些什么？
学校已经在2021年5月12日～14日以及5月21日向信息可能受到影响的 UC 社区成员发送电子邮件。请检查您的收件箱和/或垃圾邮件文件夹，查看您是否有收到该信件。发出通知的益博睿电子邮件地址是“no-reply@marketing.csid.com”，并且有说明加利福尼亚大学是发件人。那封电子邮件应该有包含一个激活代码。

如果您没有收到激活代码，请联系益博睿。我们已经成立专门的接线中心，可在星期一到星期五早上6点至晚上8点（太平洋时间）以及星期六和星期日早上8点至下午5点（太平洋时间）拨打美国国内的免费电话 (866) 904-6220。

44. 如果我之前有注册获得信用监测和身份盗窃保护，我是否需要因为 Accellion 事件再次注册？
不需要那么做。

45. 该一年信用监测和身份盗窃保护到期后，会发生什么？
学校承担一年信用监测和身份盗窃保护的费用。如果您希望在此之后继续该服务，您可以在这段时间过后购买这些服务。

46. 我丢失了学校发出的那封原始电子邮件提供的代码。我怎样获得另外一个？
如果您丢失了您的激活代码，请联系益博睿。我们已经成立专门的接线中心，可在星期一到星期五早上6点至晚上8点（太平洋时间）以及星期六和星期日早上8点至下午5点（太平洋时间）拨打美国国内的免费电话 +1 (866) 904-6220。

47. 我是否应该期待从学校获得任何关于 Accellion 事件的进一步沟通？
否。您不应该期待收到关于 Accellion 事件的任何进一步沟通。