VOLUME I, ISSUE 1 | OCTOBER 2020

COMPLIANCE MATTERS.

News and Insights from Chapman's Department of Institutional Compliance and Internal Audit

IN THIS ISSUE

Introducing Compliance Matters: What to Expect Here

By Gail Nishida, Chief Compliance Officer

Welcome to the **Compliance Matters Newsletter, Volume One**! We're excited to present to you the latest and greatest from Chapman's Department of Institutional Compliance.

In this newsletter, you can expect to find the following:

- Tidbits and information about our department and compliance-related issues
- Reminders on trainings and tools you'll need
- Guest appearances from other Chapman entities

Regardless of who you are, **Compliance is an issue that affects everyone, at every level**. From Faculty, to Students and Staff, we hope this newsletter can be a source of information, clarity and interest as we pursue the highest standards of ethical conduct here at Chapman University.

Thanks for sticking around and happy reading!

Let's Talk EthicsPoint: What You Need to Know

By Department of Institutional Compliance

Even as one of the most important reporting tools to know, EthicsPoint often goes under the radar with Faculty and Staff.

If you've never heard of EthicsPoint or don't know how it works, here's a quick refresher on what it is and when to use this awesome tool.

In simplest terms, EthicsPoint is an anonymous and confidential reporting tool for Faculty and Staff to report misconduct and violations of University policy.

From Academic Misconduct, to Conflict of Interest or Fraudulent Activities, EthicsPoint functions as a middleman to help Chapman practice the highest level of ethical conduct.

It's important to note, however, that EthicsPoint *shouldn't* override existing reporting methods such as your immediate supervisor or Human Resources. Immediate threats should also be directed to 911, *not* EthicsPoint.

If you're interested in filing a report with EthicsPoint, head over to our website at chapman.edu/compliance for directions on how to file or details on what constitutes as misconduct.

Reminder: Don't Forget About Ethics Training!

If you haven't yet already, don't forget to complete your ethics training! All Faculty (Full/Part-Time), Staff and Administrators must undergo training annually, as mandated by President Struppa. Your training invites are assigned by HR and will come through EverFi. If you have any questions regarding this process, reach out to us at compliance@chapman.edu

Guest Corner: Cyber Awareness for Fall Semester

By George Viegas, Chief Information Security Officer

As we begin the Fall 2020 semester it is important to sharpen our cyber street smarts and stay up-to-date on our cyber awareness. Malicious cyberactivity tends to increase during times when schools are re-opening and that is why we must constantly remain vigilant and cyberaware as we begin the semester remotely.

One of the most common methods used by cyber attackers to extort money from their victims is called **Ransomware**. This is when attackers, who have used phishing to gain access to your username and password, take over your computer hard drive by encrypting all the data, so you no long have access to it unless you pay a ransom.

Another common reason for cyberattacks is **identity theft**.

The cyber attackers will obtain user account credentials like login and passwords using phishing email methods, publicly available data breach information, or from hacking into data brokers. They then use the stolen credentials for malicious identity theft activities. Identity theft usually involves stolen identity records that include a consumer's name, date of birth, Social Security number, email and physical address. These identity records are then used for filing fraudulent tax return or creating fraudulent bank accounts or credit (cont.)

cards in the name of the breach account holders. The top identity theft thieves are known to make as much as $125,000/month running their business identity services selling stolen identities

So, what can we do to stay safe online? There are a few simple ways that we can continue to protect our sensitive data (private and professional):

1. **Be very cautious when opening attachments or URL links in emails.** If the email seems suspicious, please follow the below steps:

   Step 1: The Chapman security team regularly posts updates on phishing emails targeting the Chapman Community. Please check out the 'Latest security alerts' section at chapman.edu/security. If you do not see the phishing email on the security alert page, then

   Step 2: Please report the email as phishing to our Information Security team by forwarding it as an attachment (press ctrl-alt-F in Outlook to forward) to abuse@chapman.edu

2. **Use a strong password that is not easy to crack.** In this case we would recommend using a passphrase as it will increase the complexity of your password as well as make it easier for you to remember.
3. **Register your Chapman account on Microsoft's Two-Factor Authentication (2FA).** 2FA provides an extra layer of protection against unauthorized users from accessing your account even if your username and password are compromised. For directions on how to enable two-factor authentication on your Chapman account, visit the 2FA resource page.

For more information about Information Security and Cyber Safety at Chapman University, please visit chapman.edu/security