MARICOPA COMMUNITY COLLEGES | Office of the General Counsel
Compliance

MULTI-FACTOR AUTHENTICATION FOR STUDENTS AND THE SAFEGUARDS RULE

This month's Melissa Talks will cover a topic that has probably not registered on your radar. Today we are talking about the Gramm-Leach-Bliley Act (GLBA), specifically the 2022 Safeguards Rule that have an implementation date of December 9, 2022. We will focus a bit of time on multi-factor authentication for students, but let's start out by talking about the law itself.

The official title of the law at issue is the Financial Modernization Act of 1999. Among other things, the law establishes privacy and safeguarding rules regarding how financial institutions use and collect Personally Identifiable Information from their customers. The Safeguards Rule was first promulgated in 2002 and had progressive implementation deadlines. The rules we will discuss went into effect January 10, 2022 with a deadline of December 9, 2022 for implementation. The Safeguards Rule requires financial institutions to store sensitive customer information securely and ensure its secure transmission, as well as maintain programs and implement audit procedures that prevent unauthorized access and improper disclosure.

So, how does this affect the District?

The Federal Trade Commission has determined that most institutions of higher education are "financial institutions" for purposes of the GLBA because "[m]any, if not all, such institutions appear to be significantly engaged in lending funds to consumers." Moreover, the U.S. Department of Education has said Title IV schools are financial institutions subject to the legal obligations to protect student information required under the GLBA. So, the long and short of it is that the District must comply with the new Safeguards Rule.

Are there current risks at the District?

In a recent meeting with college CIOs, the following information was shared to outline just how vulnerable data is at the District. The average daily number of events that are blocked by the network firewall is 73,415. In terms of data loss prevention, there have been 124,914 security events related to data loss prevention monitored and evaluated by automated systems. All of these events relate to student/staff data on District Systems. There are also, on average, 5.6 million emails automatically blocked or filtered by Google annually. Finally, since February 2022 (when blocks were put in place), **6,433,675,056** access attempts to MCCCD systems from Russia have been blocked by our Internet firewalls. Clearly, there is a need to secure data at the District and our colleges.

What are the requirements under the Safeguards Rule that go into effect in December of 2022?

In order to answer this question, there needs to be an explanation of how the District and its colleges manage information technology. For many years, the Maricopa County Community College District has embraced a hybrid technology model that involves both centralized and decentralized decision-making, budget, procurement, and management approaches to its technology services. For example, the District ITS manages the following technologies: SIS, HCM, FMS, Duo, to name a few. The colleges locally manage the following technology such as ConexEd, Ocelot, ID badge systems, phone systems, to name a few. As a result, each college will have to address various components of the new requirements. Now, let's talk about what the rules require.

First, the District and each college must designate one employee to coordinate its information security program. This will likely be the CIO for each college and a member of the District's ITS leadership. Second, each college and the District will need to identify and assess the risks to student/employee information in each relevant area of the college or District's operation, and evaluate the effectiveness of the current safeguards for controlling these risks. The District and each college will need to design and implement a safeguards program, and regularly monitor and test it. In addition, the District and each college will need to select service providers that can maintain appropriate safeguards, make sure the contracts require them to maintain safeguards, and oversee their handling of customer information; and the District and each college will need to evaluate and adjust the program in light of relevant circumstances, including changes in the business or operation, or the results of security testing and monitoring.

How is compliance verified?

GLBA compliance has been audited each year as of FY2019. All 10 Maricopa colleges had GLBA compliance audit findings in FY2019 and FY2020 (GLBA and privacy findings are referred to the Federal Trade Commission). After a corrective action plan, there were no GLBA-related findings for FY2021. We anticipate GLBA Safeguards Rules 2022 will be part of the FY2023 audit. The consequences of non-compliance are quite serious. First, there is the threat of audit findings/repeated audit findings, which leads to a referral to the FTC for review and penalties. Federal Student Aid's Postsecondary Institution Cybersecurity Team could disable access to the Department of Education's information system (making required enrollment reporting impossible). There could be the imposition of fines and penalties up to $100,000 per violation and also criminal penalties under Section 523 of the GLBA.

What about Multi-Factor Authentication (MFA)?

MFA is an authentication method that requires the user to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. Multi-Factor Authentication was implemented for employees in the Spring of 2020. It is now being rolled out for students. Even though the GLBA does not state it explicitly, MFA is a great way to secure data. The GLBA states that **organizations must protect customer data under their care**. Since usernames and passwords are not secure, organizations should bolster their security with MFA. By requiring a user to submit an additional verification factor when signing into their systems, organizations add a layer of needed protection to critical systems ensuring GLBA compliance. As a hacker would need access to the second verification factor, which is typically either a device in a user's possession or something unique to the user like a biometric identifier, MFA is a useful measure that strengthens authentication and defends against password attacks. The process

to implement MFA is not going to be quick. In fact, we anticipate the roll-out to take the bulk of the Fall semester. More information will be forthcoming from the ITS department. Students will likely need assistance understanding how to enroll in MFA as well as how to address being locked out of the system (and locked out of Canvas and other LMS') due to a failure to enroll.

If you have any questions, please contact Melissa Flores at Melissa.Flores@domail.maricopa.edu or Dr. Mark Koan at Mark.Koan@domail.maricopa.edu.

References:

ITS InfoSec data 2021

The GLBA Safeguards Rule: What You Need to Know | Virtru

Do I Need Encryption and Multi-factor Authentication for GLBA Compliance? (24by7security.com)

What is Multi-Factor Authentication (MFA)? | OneLogin

Safeguards Rule | Federal Trade Commission (ftc.gov)

Melissa Flores
MARICOPA COMMUNITY COLLEGES
Interim General Counsel | Office of the General Counsel
2411 West 14th Street, Tempe, AZ 85281
Melissa.Flores@domail.maricopa.edu
https://www.maric opa.edu/
O: 480-731-8418 | M: 801-557-1657