



OHIO CREDIT  
UNION LEAGUE

**Proponent Testimony: House Bill 368**  
**House Criminal Justice Committee**  
**Cory Fleming**  
**Director, Legislative & Political Affairs, Ohio Credit Union League**

Chairman Lang, Vice Chair Plummer, Ranking Member Leland and Members of the House Criminal Justice Committee, my name is Cory Fleming and I am the Director of Legislative and Political Affairs at the Ohio Credit Union League, the state association representing the interests of Ohio's 261 federally and state-chartered credit unions. Thank you for allowing to me provide testimony in support of House Bill 368.

There are few issues that give credit unions more angst than worrying about a cyber-attack. As a holder of consumer's personal and private information, credit unions are often targeted by malicious actors looking to exploit the data for personal gain. Hence, credit unions continuously spend time and money on cyber-security defenses to minimize the likelihood of a breach. We commend the legislature for recognizing the threats cyber-attacks pose to all businesses in Ohio by passing Senate Bill 220 in the 132<sup>nd</sup> Ohio General Assembly, which provides an affirmative defense to those who proactively make investments to meet recognized industry security standards. House Bill 368 is an appropriate follow-up, as it clarifies and modernizes the law to make it easier to prosecute cases where a computer or computer network was intentionally used for a malicious purpose.

Our involvement with House Bill 368 came about due to one of our members, Desco Federal Credit Union, having trouble finding justice after a former employee attempted to breach their internal network. The CEO of the credit union, Lee Powell, could not be here today due to a board meeting, but has provided written testimony sharing the difficulty of prosecuting the individual, who perpetrated the breach, due to the lack of monetary damages inflicted on the credit union.

House Bill 368 migrates from the current "damages-based model" and instead, creates new criminal code related to electronic data theft, tampering, and manipulation. For instance, if a prosecutor can prove a person knowingly obtained electronic data without authorization and with the intent to execute a scheme to defraud, deceive, or extort, the individual could be convicted of a third-degree felony even in scenarios without significant monetary losses. The term "knowingly" is important, as it provides protection for "white hat hackers," who are paid to test online security systems. "Malware" is also holistically defined to mean a set of computer instructions that is designed or used to damage, destroy or disable a computer system. This change will no longer require the legislature to routinely modify the law to keep up with the latest technology used by hackers.

The legislation also allows a civil action to be brought against a person convicted of violating the law within two years of the violation or discovery of the damages. A court may award reasonable attorney's fees and equitable relief for any damages. We support this provision, as businesses should be able to recoup the monetary costs that follow a data-breach.

As House Bill 368 moves through the legislative process, we look forward to working with all interested parties. We would like to thank Representative Baldrige for his leadership on this issue, as well as Cyber-Ohio for their help in making us aware of model legislation.

Thank you for your time and I'm happy to answer any questions.