

Governor Carney Signs Legislation Extending Cybersecurity Protections for Delawareans

Legislation, sponsored by Representative Baumbach, requires additional notifications, free credit monitoring

NEWARK, Del. – Governor John Carney on Thursday signed into law [House Substitute 1 for House Bill 180](#), legislation that requires additional protections for Delawareans whose personal information may be compromised in a computer breach, including additional notifications and free credit monitoring services.

Representative Paul Baumbach sponsored the legislation, which passed the General Assembly with broad bipartisan support. The new law requires businesses to safeguard information, and requires businesses to provide free credit monitoring services for customers whose sensitive personal information is compromised in a cybersecurity breach. With Governor Carney's signature on Thursday, Delaware became just the second state to require businesses to provide those services, after Connecticut.



House Substitute 1 for House Bill 180, sponsored by Representative Baumbach, requires additional protections for Delawareans whose personal information may be compromised in a computer breach, including additional notifications

and free credit monitoring services.

“We live in a digital world where threats to personal information are becoming more common, and the cyber threat is one of the most serious economic challenges we face,” said **Governor John Carney**. “It makes sense to offer additional protections for Delawareans who may have their information compromised in a cybersecurity breach. At the same time, we will continue to connect businesses to training and resources that will help them safeguard and protect their data. I was also proud to sign this legislation on Thursday alongside Dr. Assanis at the University of Delaware, an institution that is helping lead innovation around cybersecurity. Thank you to Representative Baumbach for leading on this issue, and to all members of the General Assembly who voted to approve these new consumer protections.”

“We have worked with many stakeholders to perfect this cybersecurity legislation so that Delawareans will have proper consumer notifications and protections in place when there is a security breach of personal information. In our technological-driven world these data breaches have become too common and impact a wide variety of individuals. We had to find a way to address those concerns,” said **Representative Baumbach, D-Newark**. “This is a meaningful step forward in addressing these breaches so that we guarantee better protections for our residents and help them rebuild their lives after a cyber-attack. In particular, the bill focuses on notification requirements and additional help with identity theft mitigation services in cases where Social Security numbers are breached.”

House Bill 180 provides the first updates in Delaware law in more than a decade to address advances in cyber threats. The new law will require all companies doing business in Delaware

to implement and maintain reasonable security to protect personal information. Delaware is one of 14 states to impose explicit data security obligations on the private sector.

Thursday's signing ceremony was held at the University of Delaware, which offers a master's program in cybersecurity to help drive innovation. UD's Small Business Development Center also trains small businesses to identify cybersecurity threats and protect their business and customer data.

"The University of Delaware is committed to working with the state and our other partners to address the large and growing challenges of cybersecurity," said **Dr. Dennis Assanis, President of the University of Delaware**. "UD is devoting unique resources to developing and advancing technologies and solutions for a safe and resilient cyberspace by contributing our expertise in computer science, corporate governance and public policy."

"The Delaware Small Business Development Center is proud to be part of the Governor's signing of House Bill 180," said **Daniel Eliot, the Manager of Technology Business Development at UD's Small Business Development Center**. "For the last two years, we have worked closely with the state and other stakeholders, focused on providing training and resources to help Delaware's small businesses make a reasonable effort to secure their businesses. It's a matter of fact: all businesses today are technology-based businesses and are vulnerable to cyber breach. We want to be sure Delaware's businesses are technologically and behaviorally prepared to combat such attacks."

"The increase in cyberattacks and data breaches creates an imperative for Delaware to protect citizen information commonly used by criminals to perpetrate identity theft and fraud," said **James Collins, Chief Information Officer at the Delaware Department of Technology and Information**. "We all know that prevention is the best strategy and that is our main

goal. We want to be proactive so that our citizens and business community can avoid these threats.”

###