



The Intersection of Data Privacy and Employment Issues

ACC NCR Maryland Mixer

Maryland Personal Information Protection Act (PIPA)

- Went into effect in October 2022.
- Still not a “comprehensive privacy law” like California, Connecticut and Virginia– but moving closer
- Notable Changes:
 - Security procedures
 - Definition of personal information
 - Risk of harm analysis
 - Notification requirements/timing
 - AG Notice content requirements

Employee Data Breach Litigation

- Office of Personnel Management Data Breach - \$63MM total settlement – employee payouts of \$700 - \$10,000
 - **Standing** – compromise of information by bad actors creates substantial risk of injury, even absent proof of actual identity theft
- UPMC - \$3 MM total settlement – employee payouts of \$10-20
 - **Duty** - recognizes employer duty of care to safeguard payroll information employees are required to provide, even where only loss is economic
- State privacy laws may allow for statutory damages
 - California Consumer Privacy Act - \$750 per individual

Accidental Disclosure

An employee just moved from Virginia to Maryland and requests her company send her W-2 via email, rather than mailing a physical copy to her home address. A member of the payroll department emails the employee her W-2 but does not realize that he also included W-2s for 50 other employees.

Email Compromise- Fraudulent Wire Transfer

- An insurance agency noticed a policy premium payment it was expecting was late. The agency contacted the customer regarding the late payment.
- The customer advised the premium was already paid to the account provided in the wiring instructions sent via email.
- The customer provided a copy of the emailed wiring instructions, and they were sent from the actual insurance agency employee's account.
- A forensic investigation determined the insurance agency employee's email account was compromised and an unauthorized third party manipulated the invoicing instructions to reroute the payment to another account.

Ransomware with Data Exfiltration

- A manufacturing and shipping company is hit with ransomware. In the ransom note, the threat actor claims to have stolen data.
- Company leadership tells employees to stay home and wait for more information. They should not bring their computers to the office and should not log into the network. Employees are not told the outage is due to ransomware.
- Through its forensic investigation, the company confirms employee data was saved locally to transmit to its health benefits provider, and that file was stolen.
- The forensic investigation also confirmed that the company's head of IT had not implemented all of the security tools budgeted for the prior year.

Thank You



Debra Glickfeld Bang
Chief Legal Officer &
Corporate Secretary
dbang@emmes.com



Philip Feigen
Shareholder
pfeigen@polsinelli.com



Jack Blum
Shareholder
jack.blum@polsinelli.com



Caitlin Smith
Associate
casmith@polsinelli.com



What a law firm
should be.™



Polsinelli PC provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

© 2022 Polsinelli® is a registered trademark of Polsinelli PC. Polsinelli LLP in California. Polsinelli PC (Inc.) in Florida.

polsinelli.com