OFFICE OF THE
STATE AUDITOR

Privacy Alert 2024-03

Date: October 16, 2024

Subject: Mitigating Efforts in the Aftermath of Data Breaches

Introduction

The State Privacy Office received reports of a case in which Utah data breach victims were offered free credit monitoring, but if they accepted, they were automatically enrolled in marketing programs and their information was shared with other companies. Additionally, we have observed the automatic enrollment of victims in payment renewals by default once the free period expires. Opting out of or limiting such practices was burdensome and unclear, leaving victims with little control over their data in the aftermath of a breach.

Why is this a problem?

- **Loss of Control:** Victims may unknowingly allow their data to be widely shared, losing further control over how it is used, and struggling to opt out on account of the process being too challenging.
- **Higher Risk of Future Breaches:** More data disclosures increases the chances of further exposure.
- **Unwanted Marketing:** Automatically enrolling victims in marketing and paid programs exploits individuals in a vulnerable situation. This practice adds risks and stress for those already affected by a data breach, making them more likely to make decisions they would not otherwise make.

State Privacy Officer Recommendations:

- **Check Terms**: Advise your employees and the population you serve to limit data sharing when enrolling and to **opt out** of marketing and auto-renewals of payments where possible.
- **Stay Informed**: Encourage individuals to contact service providers to understand how their data will be used.
- **Work with Vendors**: Request vendors make data sharing for victims of data breach “opt-in” and disable auto-renewals by default, including this in contracts, following the “privacy by design and default” principle.

- **Enhance Clarity:** Ensure individuals are provided notices in simple language about their data usage and how to control it, with clear opt-in/out options, with opt-in being the default option.

Conclusion

Credit monitoring should assist individuals without causing additional risks. By prioritizing privacy by default and design, allowing individuals to control how their data is used, and requiring the same of the vendors they work with, governmental entities can offer better support and reduce the likelihood of future incidents. For further guidance and targeted training, please contact the State Privacy Officer.