CASE STUDY:
Exposure of Private Data

BACKGROUND

A large financial institution with customers in California just learned that thousands of customer email addresses were leaked, violating the California Consumer Privacy Act (CCPA) and jeopardizing its reputation as a premier institution. Upon further investigation, the team discovered that one or more cyber criminals gained access to the data through a group of third-party developers that were hired to work on the firm's core banking applications.

As a result of the mismanagement, the firm was in violation of the CCPA's Governance of Data Access policy (CCPA 1978.120, 1978.135) that requires personal user data to be limited to certain audiences and curtailed when individuals request it.

The firm thought it was only giving access to the necessary amount of data to get the job done, but in reality the developers had access to multiple streams of customer data that was not relevant to the app's functionality. Even though it was unintentional, the valuable, sensitive customer data was compromised, putting the firm in a precarious position.

Not only does the organization now face extensive sanctions, but they need to figure out how to prevent future data leaks to ensure that they don't get breached in the future so that they can stay in compliance with federal regulations.

CCPA AT A GLANCE

Who is protected?

Consumers (California residents that live in California for other than a temporary purpose).

What information is protected?

Personal information that can be reasonably linked to a particular consumer or household.

Security

The CCPA establishes a right of action for certain data breaches that are a result of a business's duty to implement and maintain reasonable security practices.

Right of Disclosure or Access

Consumers can request to disclose their data and to receive additional details about who has it.

Right of Data Portability

If asked, a business must provide personal information to the consumer in a readily useable format.

Responding to Rights Requested

A business must respond within 45 days after receipt of a consumer's request and must provide the requested information free of charge.

Penalties

Consumers may seek the greater of actual damages or statutory damages ranging from $100 to $750 per consumer per incident.

THE CHALLENGE

By necessity, the firm will need to continue hiring third-party developers; they need to find a way to guarantee that their customers' data is safe in someone else's hands. In order for their business to continue operating in compliance with the CCPA, the firm must not only control what data the developers can see, but also how much of it they can access. Along with that, they need proof of their compliance: an audit trail that assures regulators that they know who has seen what.

THE SOLUTION:

Privacy and Security by Design

ALTR integrates into the application, providing controls that are embedded, sitting in the critical path of the data. This not only ensures policy enforcement, but it delivers compliance which is the favored approach by regulators (CCPA 1978.150).

When the organization rolled out ALTR's Data Security as a Service (DSaaS) they were able to mitigate the risk of direct access to and consumption of their sensitive data. ALTR's data security was embedded within the application code, putting itself in the critical path between users and the data, providing visibility into the frequency and quantity of data being accessed by any person at any given time.

The setup process by the development team was easy, and once the tool was passed on to the security team, they had access to an intuitive, sophisticated ALTR portal that gave them the following tactical benefits:

1. **ALTR monitored the data access**. The firm gained insight into who saw what data, where they were, when they saw it, how much they saw, and how frequently they accessed it. These patterns were recorded in an immutable log that was stored in the ALTRchain, a private permissioned blockchain. Now able to see all data access in real time and protecting them from further sanctions, ALTR surpassed expectations for the firm's audit and compliance teams.

2. **ALTR governed the data**. Once the firm had insight into the typical patterns of data access, they began to set thresholds and rules over the direct access of customer data. First, the firm's security team used ALTR to mask all fields that the developers didn't require for the app; then they created a policy that cut off access in real time when users hit the predetermined threshold. This became the ultimate failsafe and will prevent any future breaches.

3. **ALTR protected the data**. Unlike tokenization and encryption, the data-at-rest was stored in a keyless, map-less vault otherwise known as the ALTRchain. This immutable private blockchain prevented anyone with direct database access from being able to smash-and-grab sensitive data.

So in addition to helping the firm comply with the CCPA's Governance of Data Access policy, ALTR took it a step further and also provided Reporting on Personal Data Use (CCPA 1978.100, 1978.300) and Compliance Reporting (CCPA 1978.115).

CONCLUSION

Not only did ALTR eliminate the risk of data leaks and provide peace of mind to the firm's compliance and security teams, but it also catalyzed the innovation process by allowing developers to move more quickly in creating their apps without that risk. In turn, the security team gained visibility and control over all of their sensitive data.

However, the value of ALTR's platform went far beyond just technical – the immutable log of all activity protected the firm's reputation with customers as well as from external compliance threats. As a result, customers now feel protected knowing that this security measure is being deployed, and they can rest assured that the previous leak of data has been taken care of.

As some might know firsthand, the biggest burden presented by the CCPA is its inevitable drainage of company resources. Typically, a large financial firm such as this would need to dedicate parts of compliance, security, and technology in order to adhere to the CCPA standards; but with ALTR, they can log in to a single portal to easily update permissions, access their immutable audit log, and quickly remove sensitive data from their environment to secure in the ALTRchain. It's a win for everyone: the firm ultimately saves money, the employees can spend their time focusing on innovation, and the customers can sleep at night knowing their data is protected.