oomnitza

How CCPA Changes Enterprise Technology Orchestration in Financial Services

How and why to move to complete IT clarity

TABLE OF CONTENTS:

Executive Summary:

The California Consumer Protection Act (CCPA) introduces many new challenges and risks, particularly for the banking industry. Financial services companies servicing U.S. customers are already subject to the provisions of the Graham Leach Bliley Act (GLBA). The CCPA broadens the types of data that must be protected and introduces new risks around data sharing with affiliates and third-parties which could leave the financial institution liable for breaches. This introduces new risks for Enterprise Technology Management (ETO) at financial services firms that must be addressed through improved ETO platform delivery and coordination. This paper addresses CCPA concerns and explains how the new law is driving new and more advanced ETO requirements and practices.

Introduction: A Large Increase in Risk to Financial Firms

The GLBA requires financial services companies to implement controls for risks to customer data, with a particular emphasis on information security including employee training for data handling, network and software design, information storage, and prevention, detection and response to breaches and attacks. Failure to comply may result in enforcement action by the SEC, the FTC, or state regulators. Consumers can also litigate against financial services firms under GLBA.

While exempting areas explicitly covered under GLBA as Federal laws, the CCPA broadly extends the variety of data that financial services firms must protect and track; this applies both to internal and directly collected data, as well as to third-party data appended to the records of customers or sales prospects. For example, the CCPA most likely exempts customer transaction or account information, and other information collected in the provision of financial products or services (potentially including IP addresses). However, the CCPA likely does not exempt personal information collected not in connection with the specific and actual delivery and provision of a product or service. The CCPA is also unlikely to exempt data shared with affiliates.

> "
> **As the regulatory environment tightens, ETO becomes mission critical.**
> "

As explained by the law firm Carlton Fields: "...the CCPA covers a wider range of information than does the GLBA, and financial institutions are likely to possess such data. The CCPA covers 'personal information' through an open-ended, default definition that focuses not on how the information was gathered but on its ability to identify its subject: information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

This expansion is significant. As further explained by the law firm Davis Tremaine Wright, "The CCPA defines personal information to include any data that relates to, describes, could be reasonably linked, or is capable of being associated with an individual or household. CCPA § 1798.140(o). This is the most expansive designation of protected information under any privacy or data security law, ever." In other words, financial services firms that may have designed systems and put in place technology to protect against GLBA violations will need to revisit almost everything they do to ensure CCPA coverage.

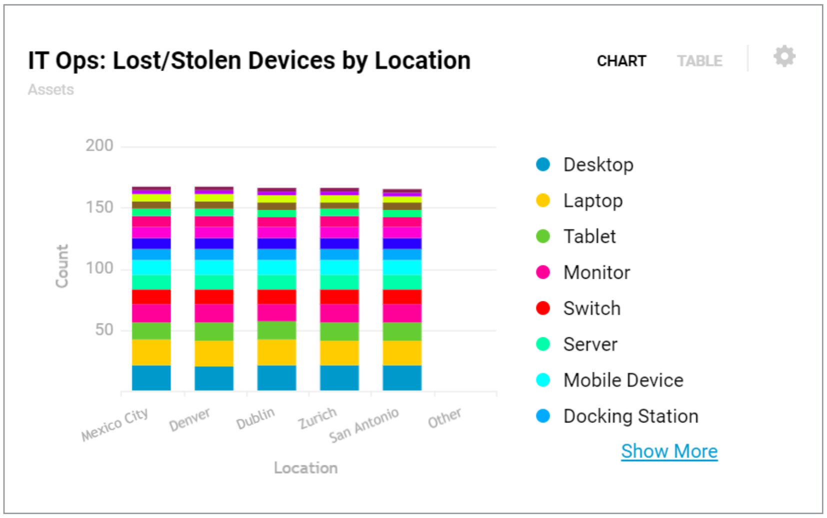
Because many financial services firms market widely, they may be protecting a mix of customer and non-customer data, often with tens of millions of records in their care. Internally, data sharing within a financial institution means CCPA compliance must cover subsidiaries and affiliates. The CCPA also broadens provisions for legal recourse for consumers who wish to sue any institution that violates the CCPA, either through its own internal fault or through an external attack that is deemed to have resulted from a failure of duty to adequately protect consumer data. This White Paper specifically addresses considerations for Enterprise Technology Orchestration with regard to financial services companies as they shore up CCPA compliance and preparation.

What is the CCPA and What Does It Cover?

The California Consumer Privacy Act (CCPA) is a broad privacy law that took effect January 1, 2020. Considered by legal experts to be among the strictest privacy laws in the United States, CCPA awards California residents sweeping powers to demand oversight as to how businesses collect, store and process any personal information. Attorneys expect CCPA to drive many new class action lawsuits: the first was filed in February 2020.

CCPA applies to any company doing business in the state of California that meets any of the these three descriptions:

- Post annual gross revenues more than $25 million
- Receives, accesses, stores or shares personal information of 50,000 or more California households, residents, or devices per year
- Accounts at least 50 percent of annual revenues from selling the personal information of California residents



> "
> **A crucial part of CCPA compliance is tracking IT assets to users and locations.**
> "

This law covers all organizations doing business in California, as well as their subsidiaries. As the law was written, companies not just in California but around the world in use by people living in California must comply with CCPA. The law focuses primarily on use of data and privacy breaches. This has specific and strong implications for enterprise technology in general, and financial service company IT asset management in particular. To underscore the importance the CCPA expands the definition of types of data the companies must protect. Some of these data types may be covered by GLBA and therefore exempted from the legal ramifications of the CCPA, depending on how, when and where consumer data is collected (e.g. - whether it is collected during specific types of a financial service company's interactions with a consumer such as account or loan applications). The long list of covered data includes:

- Social security number, military ID number and passport number
- Driver's license number and CA identification card number
- Credit or debit card number in combination with any required security code that would permit access to a consumer's financial account
- Medical information, or health insurance information
- Biometric data
- Tax identification numbers

Implications of Broad Coverage and CCPA Provisions for Enterprise Technology Orchestration

A crucial part of both enforcing CCPA compliance and reacting to any potential breaches that may have resulted in a CCPA violation is the ability to track IT assets to users and locations. We have already seen significant fines and penalties for instances where organizations lost control of IT assets, through theft or loss. For example, the University of Rochester Medical Center paid a $3 million penalty in November 2019, for failing to encrypt data on devices and systems. This fine came under the Health Insurance Portability and Accountability Act (HIPAA), which applies to healthcare organizations. CCPA allows for a maximum $7,500 penalty for each intentional violation. A smaller $2,500 penalty is possible for unintended violations. Regardless, it is unlikely that violations will be grouped together; each individual record or consumer will be considered as a violation, meaning that fines could quickly escalate into tens or hundreds of millions of dollars.

As the definition of ETO expands beyond devices and installed software to cloud infrastructure and SaaS services, CCPA serves as a forcing function for organizations to rethink and redesign their ETO strategy to better comply. Fortunately, CCPA compliance should also cover the bulk of compliance requirements for GDPR and for the patchwork of other state privacy laws either enacted or in the enactment pipeline. There is, however, a 30 day response time window under the law to report violations. If a company fails to meet this response time, then other penalties could kick in and escalate very quickly. IT and security teams for financial services companies must now respond much more quickly if there is an Indication of Compromise (IoC). Regulators are more likely to levy penalties against financial services firms due to expectations that these enterprises must be highly secure and prepared for breaches because they control such a critical component of societal infrastructure.

What Enterprise Technology Orchestration Must Deliver for CCPA Protection

Due to the broader compliance requirements introduced by CCPA, financial services institutions must improve and expand their ETO practice.

Required: A Unified View of All IT Assets

Traditionally IT asset management has included multiple disconnected data sources across hardware (ITAM), software (SAM), mobile device management (MDM) and other systems. Asset management also was siloed by operating systems (Windows, iOS, Android) and by device type (laptop and mobile, server, boxed software, SaaS / cloud infrastructure). Creating an integrated ETO capability is crucial for establishing and maintaining CCPA compliance for financial services firms. This means a single data source that acquires, reconciles and allows for easy search across all assets. The single data source works best if reconciliation and validation of assets across silos is automated, removing human error.

Why is this important? Once a breach has been identified, the clock is ticking. Invariably the first step in responding to a potential compliance violation is to identify the source and shut off or mitigate the breach or theft. This means IT and security teams need to quickly track and trace all IT assets back to users, locations, and even to IP address activity. With disconnected ITAM systems, fingerprinting the breach source is cumbersome, sometimes taking days or weeks. If those ITAM systems require manual updating, then finding and isolating the breach source is even harder; the information in the system may be weeks or months out of date and may be polluted with errors that occur in any manual information collection and updating process.

Access Of Third-Party Services Also Must Be Tracked and Auditable

In addition, the breach or violation may be caused by third-party services but exposed on the financial institutions own assets. For example, if a breach or violation is a "supply-chain" attack on a marketing service that feeds information into the databases of a bank to help them enrich marketing information, and the bank has been sharing personally identifiable information with that third-party, it is important to identify which parties inside of the bank have been accessing that service on what devices or servers in order to track the entire kill chain for compliance violations and understand the full scope of all violations.

At the time, CCPA risk (and IT asset management risk) are becoming more complex to mitigate as more assets (hardware, software, laptops/phones, Cloud, SaaS) enter the digital estate. For legacy ITAM systems tasked with tracking IT assets at every stage of their lifecycle - increasingly in near real-time - this creates significant challenges:

INABILITY OF DISCONNECTED & MANUALLY UPDATED ITAM

tools to validate the use of reasonable controls may open the door for CCPA litigation and expose legal risk

RAPID SURGES IN NUMBER AND TYPES OF DEVICES

and assets deployed due to the pandemic and work-from-home has put new pressures on all companies but particularly tightly regulated companies like financial services firms

CONTINUOUS CCPA COMPLIANCE

requires process-driven yet agile and adaptive track-and-trace of any new asset types

REDUNDANCY AND MISSING ASSETS IN

traditional ITAM systems can slow down response times

The upshot? An accurate, comprehensive cross-silo integrated ETO capability allows for more cost-effective and efficient CCPA prep and compliance. Unlike point solutions and siloed ITAMs, ETO enables automation of key discovery and reconciliation portions of CCPA prep. An ETO system also normalizes data formats across all ITAM types, creating a single database of record that is programmatically addressable and allows export of data via APIs into other systems; this is a critical component of empowering agile and adaptive track-and-trace. Ideally, ETO transforms manual CCPA compliance and prep into software code and scripts that are easy to document and generate actionable insights for better securing the IT estate against CCPA risk.

How to Achieve A CCPA-Ready ETO Capability

Here are the basic steps to upleveling ITAM to ETO for CCPA compliance and readiness.

Conduct a Bottoms Up Audit of Everything that Might Be CCPA-Facing

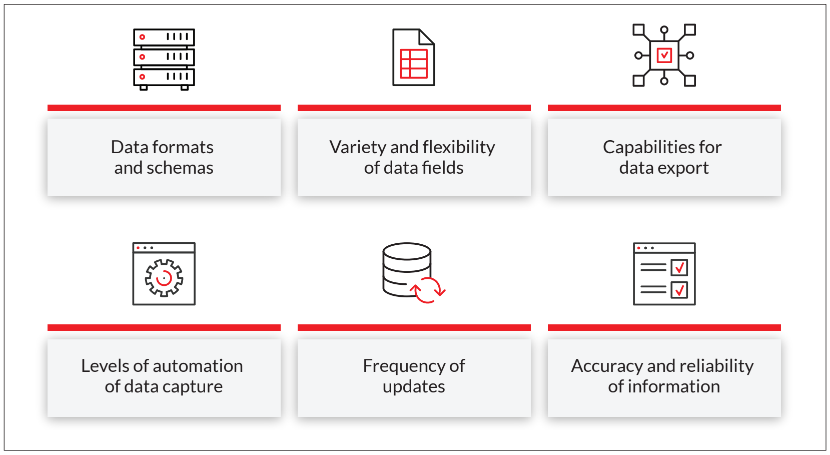
For financial service organizations to achieve comprehensive CCPA compliance with regard to IT assets, the IT and compliance team must conduct a bottoms-up and system-wide accounting of all assets under management. If this has been done previously, it is likely an updated audit is required that is broader and covers not just GLBA-impacted data. In reality, CCPA is so broad that for compliance purposes nearly all systems that contain, transmit, or analyze customer data should be considered - and by extension, all devices and assets that handle these types of data. Various ITAM systems, including CMDB, SAM, MDM, SaaS and cloud infrastructure management, manage components of what would need to be reviewed during a CCPA-prep audit.

Determine What Capabilities Are Required in Your ETO

The most important overarching questions your ETO must answer are:

- Who has access to each asset?
- Where are the assets physically and virtually located?
- Where has the asset been in the past year?
- How are the assets secured and what controls are in place to secure each asset?

As previously noted, many organizations have multiple asset management tools and systems, each adopted to solve a specific problem (e.g. hardware vs. software). For the most part, different tools have different ways of pulling in, structuring and updating data. Many lack proper APIs and export as CSV or spreadsheets. Some have automated discovery and others require manual recording by IT personnel. Specifically, many systems have differences in:



Data formats and schemas

Variety and flexibility of data fields

Capabilities for data export

Levels of automation of data capture

Frequency of updates

Accuracy and reliability of information

ETO should be able to address these differences and provide automated data capture for all existing legacy and static asset management systems. A properly integrated ETO platform automates data capture, maps fields and schemas into a unified master database, and reconciles across siloed ITAM point solution tools to create an accurate, reliable system of record. This system makes it far simpler to prevent CCPA breaches and to quickly respond to breaches by identifying compromised assets and breach sources.

Create A CCPA Response Plan for IT Assets

IT and security teams tasked with responding to CCPA complaints should create a detailed playbook with decision trees depending on the type of asset and what types of CCPA-facing data that asset may have accessed. Financial services organizations should be able to automate a regular CCPA compliance report or create a “CCPA non-compliant” flag for assets that are lacking necessary controls or are out of compliance with the organization’s information security policies.

This plan should give a financial services organization the following benefits:

- Higher accuracy and trust across asset management systems
- Faster response times to breaches or IoCs
- Repeatable, automated processes for CCPA compliance
- Greater assurance of security controls compliance

Conclusion: CCPA Means Financial Firms Need to Rethink Compliance and Security

In this paper, we have covered details about the CCPA and why it creates so much new risk for financial services companies above and beyond the existing GLBA. We also discussed why legacy ITAM systems and platforms will struggle to deliver adequate CCPA compliance. For this reason, now is an opportune time to revisit all security and compliance policies through the lens of CCPA. IT and security teams at financial services firms should move quickly to upgrade their ITAM capabilities to provide an accurate, reconciled single Enterprise Technology Orchestration solution that incorporates data from all the sub-ITAMs and unifies all asset information into one trusted system of record. Doing this will improve CCPA compliance, reduce legal and operational risk, improve response times in case of a violation, and make it easier for IT and security teams to achieve robust compliance.