Demonstrating Compliance in the Financial Services Industry with Veriato

Veriato

www.veriato.com

The biggest challenge in ensuring data security is people.

At its core, compliance is about behavior. It's about whether your users utilize protected data sets in an appropriate manner. While most organizations focus on the establishing and assessment of the security controls around access, the true test of compliance revolves around having visibility into what users do with sensitive data after they access it – the risk of data breaches, compliance violations, and the investigations, fines, and reputational damage that comes with them, depends on it.

Malicious users whose loyalty no longer aligns with the organization can improperly access, copy, email, share, or print customer, investor, or financial data – in many cases, without the knowledge of the platform or application in use.

Veriato provides contextual user activity detail and screen recordings necessary to satisfy requirements of all mandates applicable to the financial services industry. By logging all user activity and capturing screen detail for video playback, Veriato creates an indisputable audit trail that will satisfy the evidence requirements of even the most scrutinizing auditor.

This brief discusses the challenges of safeguarding customer, investor, and financial data, and how Veriato uniquely creates the audit detail necessary to meet compliance objectives.

Introduction

Nearly all financial services companies and financial institutions are subject to a number of compliance mandates. The Gramm-Leach-Bliley Act (GLBA) and the Dodd-Frank Wall Street Reform and Consumer Protection Act both provide specific guidance on how financial services organizations need to protect consumer data within financial systems. The enforcement of these regulations is overseen by both the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB). In addition, the Sarbanes-Oxley (SOX) regulation seeks to protect investor information, but is vague when it comes to specific required activities. Those organizations processing credit card information, must also comply with the Payment Card Industry Data Security Standard (PCIDSS). Lastly, those financial services companies residing in the state of New York now must also comply with the new Cybersecurity Requirements (23 NYCRR 500), which outlines specific technical and administrative controls to be in place.

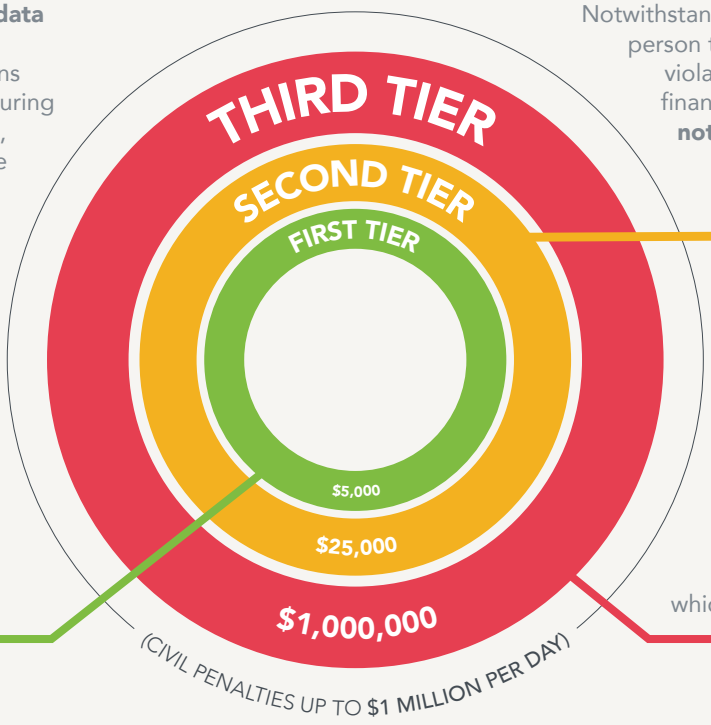
So, financial services organizations require an ability to have complete visibility into every action performed by a user with access to customer, financial, and investor data – every application used, webpage visited, record copied, file saved, print screen generated, and page printed. Only then will a covered entity truly know whether protected data has been appropriately accessed and used by either true insiders, or external attackers posing as insiders via stolen credentials.

But, compliance to GLBA, Dodd-Frank, SOX, PCI, 23 NYCRR 500 or any other mandate is as much about establishing and adhering to policies and procedures, as it is maintaining appropriate technical controls. Both are needed to confirm users have been instructed on proper access to and usage of sensitive data, access to protected data is correctly granted, use is appropriate, and compliance can be demonstrated.

There are severe penalties for non-compliance: GLBA poses imprisonment for up to 5 years, with steep fines of up to $100,000 for each violation, and up to $10,000 fines for officers and directors for each violation. Dodd-Frank poses civil penalties of up to $1,000,000 per day the organization remains in violation. Penalties for non-compliance with PCI range from $50,000 to $500,000. NYDFS' requirements tout civil penalties, but do not provide specifics.

PENALTIES

Given the fact that **24% of all data breaches target the financial services industry** , organizations face a challenge of not just ensuring internal processes are followed, but to remain secure in the face of data breaches that involve the use of stolen credentials 81% of the time[1].



Notwithstanding paragraph (A), for any person that recklessly engages in a violation of a Federal consumer financial law, a civil penalty **may not exceed $25,000 for each day** during which such violation continues.

For any violation of a law, rule, or final order or condition imposed in writing by the Bureau, a civil penalty **may not exceed $5,000 for each day** during which such violation or failure to paycontinues.

Notwithstanding subparagraphs (A) and (B), for any person that knowingly violates a Federal consumer financial law, a civil penalty **may not exceed $1,000,000** for each day during which such violation continues.

[1] Verizon, Data Breach Investigations Report (2017)

Compliance Challenges for Key Stakeholders

While most compliance mandates aren't broken out into separate specific objectives for each stakeholder in the organization, stakeholders each have different needs around the goal of adhering to any:

CEO – Needs a proactive approach leveraging people, processes, and technology that ensures adherence to mandate requirements around safeguarding protected data.

CFO – Can't afford the cost of a breach in compliance. Would rather spend budget on preventative measures, than on responding to a breach.

CCO – Wants a plan in place of how to easily and quickly demonstrate compliance.

CSO – Desires for protected data to remain secure, and a way to know protected data isn't being misused.

IT Manager – Needs to provide a means of visibility into exactly how protected data is used, regardless of application.

What's needed is a technology that cost-effectively addresses compliance requirements by monitoring the access to protected data, aligning with established policy and processes, providing visibility into how protected data is used or misused, and providing context around either demonstrating compliance or determining the scope of a breach.

Demonstrating Compliance with Veriato

The intent of each of the mentioned compliance mandates is to ultimately ensure the privacy of non-public financial, investor, and personal data. As long as the only access a given protected data is performed by someone who both has a legitimate need and only uses that information for the purposes of the organization, your organization will remain compliant. But, because users with access to protected data utilize that access every day, it becomes nearly impossible to tell if and when your organization may be out of compliance. Add to that the fact that, while the access to data may seem appropriate, the cutting and pasting of information into a Word doc saved up on a cloud drive certainly isn't – which means your organization needs to be monitoring and recording all user activity, regardless of application.

Veriato assists with establishing compliance with requirements specific to financial services organizations by providing IT, security teams, and auditors alike with complete visibility into every action taken by the organization's users. Veriato solutions help to analyze risk, audit controls, and review activity in an effort to establish, maintain, and continually demonstrate compliance.

GLBA - 15 U.S. CODE 6801 / FTC SAFEGUARDS RULE -16 CFR PART 314

Protection of Non-public personal Information

Veriato acts as a core part of your implementation and maintenance of security measures to protect personally identifiable financial information, specifically around monitoring and reviewing the conduct of you workforce in relation to the protection of non-public personal information.

Below are some examples of how Veriato can assist in addressing GLBA's requirement for administrative and technical safeguards:

- **Insure the security and confidentiality of customer records and information** – Veriato provides visibility into how users access, interact with, and use personal information. Veriato creates an audit trail used to assess whether security and confidentiality has been maintained, regardless of application used.

- **Protect against any anticipated threats or hazards to the security or integrity of such records** – By leveraging user behavior analytics, Veriato provides a contextual activity review of both the access to personal information, as well as technical and psycholinguistic indicators to provide an early warning of threats.

DODD-FRANK - SECTION 154(B)(3), ORGANIZATIONAL STRUCTURE; RESPONSIBILITIES OF PRIMARY PROGRAMMATIC UNITS – DATA CENTER

Information Security

While broad in scope, this section intends that processes, policy, and technology be put in place to ensure financial data is "kept secure and protected against unauthorized disclosure." Veriato's advanced user activity monitoring and behavior analysis technology monitors and can alert the Council or Director (as defined within the Act) of inappropriate access to protected data, regardless of application.

Below are some examples of how Veriato can assist in addressing this requirement, include:

- **Notification of Unauthorized Disclosure** – Before disclosure can be made, an assessment of the scope of the unauthorized access must be determined. Veriato not only empowers security teams to record an examine user activity within systems containing protected financial data, but also within any other application, providing unmatched visibility into actions taken around financial data access. Should users attempt to copy, print, email, instant message, etc. financial data, Veriato is immediately aware of it and can notify the proper authorities.

SARBANES-OXLEY ACT – SECTIONS 302 & 404

Internal Control Assessment

While SOX does little in the area of providing specific guidance around what internal controls are necessary to ensure the accuracy of financial reporting, section 302 establishes the signing officer is responsible for such controls, and section 404 requires an annual internal control report

Below are some examples of how Veriato can assist in addressing Sarbanes-Oxley requirements:

- **Internal Control Assessment** – The simplest means of assessing internal controls is to observe their practical application, looking for misuse by users or acts of fraud. Veriato's comprehensive visibility into all user activity across applications empowers organizations to assess the state of controls, ensuring only approved users are accessing protected data, and providing contextual detail around any activity that may put the integrity of financial reporting into question.

NEW YORK STATE DFS – 23 NYCRR 500

Cybersecurity Requirements for Financial Services Companies

New York State has implemented its own additional set of requirements for financial services companies to ensure the integrity and confidentiality of non-public personal and financial information.

Below are a few examples of where Veriato can assist in meeting these new requirements:

- **Audit Trail (500.06)** – Veriato's unmatched ability to record activity across every application facilitates a comprehensive audit trail, providing complete visibility into all user actions.
- **Risk Assessment (500.09)** – Veriato's activity data and reporting provide necessary activity detail that provide context as part of an overall risk assessment, identifying any means by which users have been able to inappropriately access and/or misuse non-public data.
- **Monitoring of Authorized Users (500.14)** – User activity is constantly being recorded with Veriato, where unauthorized access to, misuse of, or tampering with non-public data can be defined, monitored, and alerted upon.
- **Incident Response Plan (500.16)** – Should non-public data be accessed, misused, or tampered with.

How Veriato Helps Address Compliance Challenges

Veriato helps financial services organizations of all kinds satisfy their compliance obligations through detailed, contextual, rich logging of all user activity – both inside systems housing financial, customer, or investor data, as well as any other application – combined with robust screen recording and playback. This level of visibility into user interaction with protected data provides comprehensive evidence for compliance audits. Activity data is searchable, making it easy for an auditor, security teams, or IT to find suspect actions, with the ability to playback activity to see before, during, and after the activity in question. Reports can be produced in minutes – typically a fraction of the time needed – and don't require pulling critical resources from other tasks.

Veriato assists in meeting a number of specific requirements, leveraging its deep visibility into user activity to provide context around access to protected data, showing what was accessed and what was done with the data. The following sections outline how Veriato can assist with meeting specific compliance requirements.

To learn more about how Veriato can help you with Financial Services Compliance, contact a Veriato representative today

Our solutions are deployed in 110+ countries

Over 3,000 enterprises, & thousands of SMBs have placed their trust in our solutions

Veriato
www.veriato.com

Veriato USA
4440 PGA Boulevard , Suite 500
Palm Beach Gardens, FL 33410

Veriato EMEA
3rd Floor, Crossweys House
28-30 High Street
Guildford, Surrey
GU1 3EL United Kingdom

https://www.linkedin.com/company/veriato
https://twitter.com/veriato
https://www.facebook.com/VeriatoInc/