MAPPING GUIDE

Mapping to PCI DSS 3.2.1, requirement 10

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

According to the Verizon 2018 Payment Security Report, "not only is compliance with Requirement 10 (Monitoring) a consistent problem across breached organizations, it has the dubious honor of being the only Requirement with a negative trendline across breached organizations."

Section	PCI DSS 3.2.1 Requirements	Testing Procedures	Guidance	Imprivata FairWarning Capabilities
10.1	10.1 Implement audit trails to link all access to system components to each individual user.	10.1 Verify, through observation and interviewing the system administrator, that: • Audit trails are enabled and active for system components. • Access to system components is linked to individual users.	It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.	Imprivata FairWarning Analytics record and examine all user's access to and activity with any system components. These Analytics are then automated as Enforced Policies to proactively alert users of any activity that is being tracked or audited.
10.2	10.2 Implement automated audit trails for all system components to reconstruct the following events.	10.2 Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following:	Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post- incident follow-up. Logging of the following events enables an organization to identify and trace potentially malicious activities.	Imprivata FairWarning Analytics and Reports enable reviewing of information system activity such as audit logs and access reports to reconstruct the required events. Imprivata FairWarning Investigations centralize management and tracking of these events and security incidents.

Section	PCI DSS 3.2.1 Requirements	Testing Procedures	Guidance	Imprivata FairWarning Capabilities
10.2.1	10.2.1 All individual user accesses to cardholder data.	10.2.1 Verify all individual access to cardholder data is logged	Malicious individuals could obtain knowledge of a user account with access to systems in the CDE, or they could create a new, unauthorized account in order to access cardholder data. A record of all individual accesses to cardholder data can identify which accounts may have been compromised or misused.	Imprivata FairWarning Analytics record and examine user activity, including any access to cardholder data. These Analytics are then automated as Enforced Policies to proactively alert users of any activity that is being tracked or audited.
10.2.2	10.2.2 All actions taken by any individual with root or administrative privileges.	10.2.2 Verify all actions taken by any individual with root or administrative privileges are logged.	Accounts with increased privileges, such as the “administrator” or “root” account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual.	Imprivata FairWarning Analytics record and examine all user’s activity, regardless of their system permissions and privileges. These Analytics are then automated as Enforced Policies to proactively alert users of any activity that is being tracked or audited.
10.2.3	10.2.3 Access to all audit trails.	10.2.3 Verify access to all audit trails is logged	Malicious users often attempt to alter audit logs to hide their actions, and a record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account. Having access to logs identifying changes, additions, and deletions can help retrace steps made by unauthorized personnel.	Imprivata FairWarning Analytics and Reports enable reviewing of information system activity, including access to the audit logs themselves. These Analytics are then automated as Enforced Policies to proactively alert users of any activity that is being tracked or audited.
10.2.4	10.2.4 Invalid logical access attempts.	10.2.4 Verify invalid logical access attempts are logged.	Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user’s attempts to “brute force” or guess a password.	Imprivata FairWarning Analytics record and examine all user’s activity, including their login successes, failures, and attempt locations. These Analytics are then automated as Enforced Policies to proactively alert users of any activity that is being tracked or audited.

Section	PCI DSS 3.2.1 Requirements	Testing Procedures	Guidance	Imprivata FairWarning Capabilities
10.2.5	10.2.5 Use of and changes to identification	10.2.5.a Verify use of identification and authentication mechanisms is logged. 10.2.5.b Verify all elevation of privileges is logged. 10.2.5.c Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.	Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.	Imprivata FairWarning Analytics record and examine all user's activity, including any modifications to any user information or privileges. These Analytics are then automated as Enforced Policies to proactively alert users of any activity that is being tracked or audited.
10.2.6	10.2.6 Initialization, stopping, or pausing of the audit logs	10.2.6 Verify the following are logged: Initialization of audit logs Stopping or pausing of audit logs.	Turning the audit logs off (or pausing them) prior to performing illicit activities is a common practice for malicious users wishing to avoid detection. Initialization of audit logs could indicate that the log function was disabled by a user to hide their actions	Reference your application provider's auditing capabilities such as Salesforce Event Monitoring.
10.2.7	10.2.7 Creation and deletion of system level objects	10.2.7 Verify creation and deletion of system level objects are logged.	Malicious software, such as malware, often creates or replaces system level objects on the target system in order to control a particular function or operation on that system. By logging when system- level objects, such as database tables or stored procedures, are created or deleted, it will be easier to determine whether such modifications were authorized.	Imprivata FairWarning Analytics and Reports enable reviewing of information system activity, including any modification to standard and custom system objects. These Analytics are then automated as Enforced Policies to proactively alert users of any activity that is being tracked or audited.
10.3	10.3 Record at least the following audit trail entries for all system components for each event:	10.3 Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following:	By recording these details for the auditable events at 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how.	Imprivata FairWarning Analytics and Reports enable reviewing of information system activity such as audit logs and access reports. Imprivata FairWarning® Investigations allows you to centralize, manage, and track all security incidents.

Section	PCI DSS 3.2.1 Requirements	Testing Procedures	Guidance	Imprivata FairWarning Capabilities
10.3.1	10.3.1 User identification.	10.3.1 Verify user identification is included in log entries.		Imprivata FairWarning Analytics and Reports enable reviewing of information system activity, including detailed user information and identification.
10.3.2	10.3.3 Date and time.	10.3.3 Verify date and time stamp is included in log entries.		Imprivata FairWarning Analytics and Reports enable reviewing of information system activity, including exact date and time stamps.
10.3.3	10.3.3 Date and time.	10.3.3 Verify date and time stamp is included in log entries.		FairWarning Analytics and Reports enable reviewing of information system activity, including exact date and time stamps.
10.3.4	10.3.4 Success or failure indication.	10.3.4 Verify success or failure indication is included in log entries.		Imprivata FairWarning Analytics and Reports enable reviewing of information system activity, including success or failure in accordance with the type of action or activity attempted.
10.3.5	10.3.5 Origination of event.	10.3.5 Verify origination of event is included in log entries.		Imprivata FairWarning Analytics and Reports enable reviewing of information system activity, including the location and origination of the activity.
10.3.6	10.3.6 Identity or name of affected data, system component, or resource.	10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.		Imprivata FairWarning Analytics and Reports enable reviewing of information system activity, including any modification to standard and custom system objects as well as fields. These Analytics are then automated as Enforced Policies to proactively alert users of any activity that is being tracked or audited.

Section	PCI DSS 3.2.1 Requirements	Testing Procedures	Guidance	Imprivata FairWarning Capabilities
10.5	10.5 Secure audit trails so they cannot be altered.	10.5 Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows:	Often a malicious individual who has entered the network will attempt to edit the audit logs in order to hide their activity. Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a compromise.	Imprivata FairWarning secures, stores and archives audit trails from applications in accordance with the customer's regulatory requirements including PCI DSS 3.2.1.
10.5.1	10.5.1 Limit viewing of audit trails to those with a job-related need.	10.5.1 Only individuals who have a job-related need can view audit trail files.	Adequate protection of the audit logs includes strong access control (limit access to logs based on "need to know" only), and use of physical or network segregation to make the logs harder to find and modify. Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected even if the system generating the logs becomes compromised.	Role-based access control is built in to all Imprivata FairWarning® solutions that can be configured through a point and click interface to meet a customer's regulatory and security requirements.
10.5.2	10.5.2 Protect audit trail files from unauthorized modifications.	10.5.2 Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.		Imprivata FairWarning secures, stores and archives audit trails from applications in accordance with the customer's regulatory requirements including PCI DSS 3.2.1.
10.5.3	10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	10.5.3 Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.		Imprivata FairWarning® secures, stores and archives audit trails from applications in accordance with the customer's regulatory requirements including PCI DSS 3.2.1.

Section	PCI DSS 3.2.1 Requirements	Testing Procedures	Guidance	Imprivata FairWarning Capabilities
10.5.4	10.5.4 Write logs for external-facing technologies onto a log server on the internal log server or media device.	10.5.4 Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media.	By writing logs from external-facing technologies such as wireless, firewalls, DNS, and mail servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network. Logs may be written directly, or offloaded or copied from external systems, to the secure internal system or media.	The production of the logs as described in this requirement are satisfied by each respective vendor's auditing subsystem such as Salesforce Event Monitoring, infrastructure and security devices.
10.5.5	10.5.5 Use file integrity monitoring or change- detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	10.5.5 Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs.	File-integrity monitoring or change-detection systems check for changes to critical files, and notify when such changes are noted. For file- integrity monitoring purposes, an entity usually monitors files that don't regularly change, but when changed indicate a possible compromise.	Imprivata FairWarning® secures, stores and archives audit trails from applications in accordance with the customer's regulatory requirements including PCI DSS 3.2.1.

Section	PCI DSS 3.2.1 Requirements	Testing Procedures	Guidance	Imprivata FairWarning Capabilities
10.6	10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	10.6 Perform the following:	Many breaches occur over days or months before being detected. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the cardholder data environment. The log review process does not have to be manual. The use of log harvesting, parsing, and alerting tools can help facilitate the process by identifying log events that need to be reviewed.	Imprivata FairWarning Analytics and Reports enable reviewing of information system activity such as audit logs and access reports. These Analytics are then automated as Enforced Policies to proactively alert users of any activity that is being tracked or audited. These Enforced Policies and alerts can then be used to create an Investigation which can be centrally managed, reviewed, and tracked along with all other security incidents and investigations.

Section	PCI DSS 3.2.1 Requirements	Testing Procedures	Guidance	Imprivata FairWarning Capabilities
10.6.1	10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/ or SAD. • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	10.6.1.a Examine security policies and procedures to verify that procedures are defined for reviewing the following at least daily, either manually or via log tools: • All security events • Logs of all system components that store, process, or transmit CHD and/ or SAD. • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/ intrusion-prevention systems (IDS/ IPS), authentication servers, e-commerce redirection servers, etc.) 10.6.1.b Observe processes and interview personnel to verify that the following are reviewed at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/ or SAD, or that could impact the security of CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/ intrusion-prevention systems (IDS/IPS), authentication servers, e- commerce redirection servers, etc.).	Checking logs daily minimizes the amount of time and exposure of a potential breach. Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. is necessary to identify potential issues. Note that the determination of “security event” will vary for each organization and may include consideration for the type of technology, location, and function of the device. Organizations may also wish to maintain a baseline of “normal” traffic to help identify anomalous behavior.	Imprivata FairWarning centralizes where and how applications are audited. All systems touching cardholder data can be audited through the Imprivata FairWarning® Analytics and Reports. These audits can be automated as Enforced Policies and all investigations can be centrally managed within the product. Governance and dashboard reports give executive views of the effectiveness of the policies being enforced.

Section	PCI DSS 3.2.1 Requirements	Testing Procedures	Guidance	Imprivata FairWarning Capabilities
10.6.2	10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	10.6.2.a Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically— either manually or via log tools—based on the organization's policies and risk management strategy. 10.6.2.b Examine the organization's risk- assessment documentation and interview personnel to verify that reviews are performed in accordance with organization's policies and risk management strategy.	Logs for all other system components should also be periodically reviewed to identify indications of potential issues or attempts to gain access to sensitive systems via less-sensitive systems. The frequency of the reviews should be determined by an entity's annual risk assessment.	Imprivata FairWarning assists customers in addressing one of the most common risk areas identified during a risk assessment: insider misuse of access to cardholder data. Imprivata FairWarning has many materials available to help you make the best use of user activity monitoring, and therefore reduce your risk.
10.6.3	10.6.3 Follow up exceptions and anomalies **identified during the review process.**	10.6.3.a Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. 10.6.3.b Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed.	If exceptions and anomalies identified during the log- review process are not investigated, the entity may be unaware of unauthorized and potentially malicious activities that are occurring within their own network.	Imprivata FairWarning Analytics and Reports enable reviewing of information system activity such as audit logs and access reports. These Analytics are then automated as Enforced Policies to proactively alert users of any activity that is being tracked or audited. These Enforced Policies and alerts can then be used to create an Investigation which can be centrally managed, reviewed, and tracked along with all other security incidents and investigations.

Section	PCI DSS 3.2.1 Requirements	Testing Procedures	Guidance	Imprivata FairWarning Capabilities
10.7	10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	10.7.a Examine security policies and procedures to verify that they define the following: • Audit log retention policies • Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. 10.7.b Interview personnel and examine audit logs to verify that audit logs are available for at least one year. 10.7.c Interview personnel and observe processes to verify that at least the last three months' logs can be immediately restored for analysis.	Retaining logs for at least a year allows for the fact that it often takes a while to notice that a compromise has occurred or is occurring, and allows investigators sufficient log history to better determine the length of time of a potential breach and potential system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach. Storing logs in off-line locations could prevent them from being readily available, resulting in longer time frames to restore log data, perform analysis, and identify impacted systems or data.	Imprivata FairWarning secures, stores and archives audit trails from applications in accordance with the customer's regulatory requirements including PCI DSS 3.2.1, Requirement 10.7.
10.8	10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures for the critical security control systems, including but not limited to the failure of:	10.8.a Examine documented policies and processes to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) 10.8.b Examine detection and alerting processes to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	**Note: This requirement applies only when the entity being assessed is a service provider.** Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the cardholder data environment. The specific types of failures may vary depending on the function of the device and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner; for example, a firewall erasing all its rules or going offline.	Imprivata FairWarning has documented policies and processes in place to monitor, correct (as needed) and report on its critical security control systems.

Section	PCI DSS 3.2.1 Requirements	Testing Procedures	Guidance	Imprivata FairWarning Capabilities
10.8.1	10.8 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include:	10.8.1.a Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include: • Restoring security functions • Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether future actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls 10.8.1.b Examine records to verify that security control failures are documented to include: • Identification of cause (s) of the failure, including root cause • Duration (date and time start and end) of the security failure • Details of the remediation required to address the root cause	**Note: This requirement applies only when the entity being assessed is a service provider.** If critical security control failures alerts are not quickly and effectively responded to, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment. Documented evidence (e.g., records within a problem management system) should support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.	Imprivata FairWarning has documented policies and processes in place to monitor, correct (as needed) and report on its critical security control systems. Its staff receive regular education, and testing, on how to respond to failures within any critical security controls.

Section	PCI DSS 3.2.1 Requirements	Testing Procedures	Guidance	Imprivata FairWarning Capabilities
10.9	10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	10.9 Examine documentation and interview personnel to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are: • Documented, • **In use, and** • **Known to all affect parties**	Personnel need to be aware of and following security policies and daily operational procedures for monitoring all access to network resources and cardholder data on a continuous basis.	Imprivata FairWarning centralizes where and how applications are audited. All systems touching cardholder data can be audited through the Imprivata FairWarning Analytics and Reports. These audits can be automated as Enforced Policies and all investigations can be centrally managed within the product. Governance and dashboards give customers a way to document the effectiveness of the policies being enforced and engage staff in ongoing security education (and correction as needed).