BriteStar

NADA Compliance Requirements
BriteStar & BriteProtect

DealerDOCX
DOCUMENT INTELLIGENCE

Brite

Safeguard Rules

1. Appointment of a "Qualified Employee"

Currently, dealers must designate an "employee or employees to coordinate your information security program."

The Amended Rule instead requires dealers to designate "a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program."

Brite Service Offering

Virtual CISO services – documentation, planning, oversight.

2. Requirement to undertake a written "Risk Assessment"

The Amended Rule requires that a new written document—a "Risk Assessment"—be drafted, and that it must contain and address certain areas of risk at the financial institution.

Brite Service Offering

Annual risk assessment, quarterly assessment progress review

3. Implementation of "Access Controls"

The Amended Rule requires dealers to "place access controls on information systems, including controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of customer information and to periodically review such access controls."

Brite Service Offering

Multi-factor authentication, identity access management, access anomaly detection

4. Undertake a required data and systems inventory

The Amended Rule requires dealers to "identify and manage the data, personnel, devices, systems, and facilities that enable [the financial institution] to achieve business purposes in accordance with their relative importance to business objectives and [the financial institution's] risk strategy."

Brite Services Offering
Asset management services and data monitoring

5. Data encryption requirement

The Amended Rule requires dealers to "encrypt all customer information, both in transit over external networks and at rest." This requirement also extends to all dealer vendors and others with access to dealership customer data.

Brite Services Offering
Full-disk encryption on laptops and servers, email protection including data loss prevention and encryption.

6. Requirement to adopt secure development practices and assess externally developed applications

The Amended Rule requires dealers to "adopt secure development practices for in-house developed applications utilized" for "transmitting, accessing, or storing customer information" and requires "procedures for evaluating, assessing, or testing the security of externally developed applications [financial institutions] utilize to transmit, access, or store customer information."

Brite Offered Services
Weekly vulnerability testing, annual penetration testing, Dev/Sec/Ops – code scanning

7. Multi-factor authentication

The Amended Rule requires dealers to "implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls." Again, this requirement applies equally to service providers that house or access dealership data or systems.

Brite Service Offering
Multi-factor authentication, identity access management, access anomaly detection

8. Systems monitoring and logging

The Amended Rule requires dealers to "implement policies, procedures and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users."

Brite Service Offering

BriteProtect Managed Security Operation Center as a Service/SOCaaS (XDR)

9. Development of secure data disposal procedures

The Amended Rule requires dealers to "develop, implement, and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation, or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained."

Brite Service Offering

Secure device disposal, data retentions (all tools)

10. Required change management procedures

The Amended Rule requires dealers to "to adopt procedures for change management" which "govern the addition, removal, or modification of elements of an information system."

Brite Service Offering

Virtual CISO (Information Security Plan documentation creation, adherence, assessment completion and planning, policy creation and oversight)

11. Required unauthorized activity monitoring

The Amended Rule requires dealers to implement policies and procedures designed "to monitor the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users."

Brite Service Offering

BriteProtect Managed Security Operation Center as a Service/SOCaaS (XDR), requires monitoring tools for systems (applications, email, web, etc.)

12. Required intrusion detection and vulnerability testing

The Amended Rule requires dealers to "regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems."

Brite Service Offering

Vulnerability management (continuous), penetration testing (annual)

13. Series of new requirements to ensure that personnel are able to enact the information security program

The Amended Rule also includes a series of requirements intended to ensure that the dealer has the appropriate personnel to adequately protect and secure data and that those personnel are able and qualified to enact the dealership's security program.

These include:

- General employee training
  The Amended Rule requires dealers to "provide their personnel with "security awareness training that is updated to reflect risks identified by the risk assessment."
- The use of qualified information security personnel
  The Amended Rule requires dealers to "utilize qualified information security personnel," employed either by them or by affiliates or service providers, "sufficient to manage [their] information security risks and to perform or oversee the information security program."
- Specific training for information security personnel
  The Amended Rule requires dealers to "provide information security personnel with security updates and training sufficient to address relevant security risks." This requirement is separate and in addition to the "general training" requirement above.
- Verification that security personnel are taking steps to maintain current knowledge on security issues
  Finally, under this section, the Amended Rule requires dealers to ""verify that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures." The FTC states that "this requirement was intended to complement the proposed requirement regarding ongoing training of data security personnel, by requiring verification that such training has taken place."

Brite Service Offering

Team of BriteProtect experienced personnel, user awareness training and simulation for employees penetration testing including social engineering

14. Overseeing and monitoring service providers

The Amended Rule also requires dealers to "Oversee service providers, by: Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; Requiring service providers by contract to implement and maintain such safeguards; and periodically assessing service providers, based on the risk they present and the continued adequacy of their safeguards."

This requirement is similar to existing requirements regarding service providers, except that it also expressly contains a requirement to monitor and assess service providers after the onboarding stage. This will likely include audits and other formal and documentable assessment steps.

Brite Service Offering

SOC2 certified managed security services, 3rd party penetration testing

15. Required written incident response plan

The Amended Rule requires dealers to adopt a written incident response plan that specifically addresses: the goals of the plan;

- the internal processes for responding to a security event
- the definition of clear roles, responsibilities, and levels of decision-making authority
- external and internal communications and information sharing
- identification of requirements for the remediation of any identified weaknesses in information systems and associated controls
- documentation and reporting regarding security events and related incident response activities
- the evaluation and revision as necessary of the incident response plan following a security event

Brite Service Offering

Incident response services, incident response tabletop

16. Required annual written report to the Board

The Amended Rule requires dealers to "Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body."

This report must cover specific delineated areas, including:

- the overall status of the information security program and the dealer's compliance with the Safeguards Rule
- material matters related to the information security program addressing issues such as:
  - risk assessment
  - risk management and control decisions
  - service provider arrangements
  - results of testing
  - security events or violations and management's responses thereto
  - recommendations for changes in the information security program

Brite Service Offering

Series of reports and check lists