Locke Lord LLP

New Federal Trade Commission's Safeguards Rule is a Game-Changer for Extended Warranty and GAP Waiver Industries

By Brian T. Casey, Theodore P. Augustinos and Alexander R. Cox

The Federal Trade Commission ("FTC") has recently supercharged the Gramm-Leach-Bliley Act's Safeguards Rule for financial institutions under its jurisdiction. The Safeguards Rule imposes data security standards for consumer nonpublic person information obtained and created by financial institutions subject to the FTC's Gramm-Leach-Bliley Act jurisdiction. The FTC finalized its proposed update to the Safeguards Rule on October 28, 2021, which was originally published for rule-making in March 2019 and then further developed during an FTC workshop in July 2020. After a lengthy gestation period, the new revised rule became effective January 10, 2022, and requires compliance by December 9, 2022.

The new FTC Safeguards Rule embraces many of the core concepts of the New York Department of Financial Services Cybersecurity Regulation (23 NYCRR Part 500, the "NYDFS Cybersecurity Regulation") and the National Association of Insurance Commissioners Insurance Data Security Model Law (MDL-668, the "NAIC Data Security Model"), which has been adopted in 18 states.[1] Participants in many industries that do not provide traditional consumer financial products or services and are not overseen by a functional regulator such as the Office of the Comptroller of the Currency, the Federal Reserve or state insurance departments, but provide consumer offerings such as warranties and service contracts are subject to the FTC's jurisdiction. Many of these offerings are similar to insurance products, including consumer goods extended warranty providers. Therefore, the new FTC Safeguards Rule will require action by providers and sellers of a wide variety of consumer product protection plans, including (i) service contracts for consumer electronics and vehicles (a.k.a. "extended warranties"); (ii) service contracts covering major appliances as well as electrical, heating and cooling systems of a home (sometimes separately regulated as "home warranties"); and (iii) certain types of auto loan or lease guaranteed asset protection waivers (a.k.a. "GAP waivers"). In addition to reviewing the applicability of the FTC Safeguards Rule to providers and sellers of these products and services, this article also reviews the reviews the background of the privacy and security rules for financial institutions, and the scope of the FTC's authority.

[1] These 18 states are: Alabama; Connecticut; Delaware; Hawaii; Indiana; Iowa; Louisiana; Maine; Michigan; Minnesota; Mississippi; New Hampshire; North Dakota; Ohio; South Carolina; Tennessee; Virginia; and Wisconsin.

Locke Lord LLP

Background of Gramm-Leach-Bliley Act's Privacy and Security Regulations

The Gramm-Leach-Bliley Act ("GLBA") regulates financial institutions' collection, use and disclosure of nonpublic personal information, and requires notices to consumers of their privacy practices. The applicable governmental agency with enforcement authority over the GLBA's privacy and security requirements is generally the functional regulator of a particular type of financial institution. Indeed, the GLBA assigns rulemaking authority as follows: (a) for banks and their subsidiaries, the appropriate federal banking regulatory agency (the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, and the Board of Directors of the Federal Deposit Insurance Corporation ("FDIC")[2]); (b) for federal credit unions, the National Credit Union Administration; (c) for securities brokers and dealers, investment companies, and investment advisers, the Securities and Exchange Commission ("SEC"); (d) for persons engaged in providing insurance, the applicable state insurance authority; and (e) for any other person that is not subject to the jurisdiction of any agency or authority described above, the FTC.

Originally under the GLBA, the FTC essentially became the default GLBA privacy and security regulator for consumer financial products and services offered by financial institutions for which there was no functional regulatory agency (either federal or state) exercising oversight of such products or services. The Dodd Frank Act transferred the majority of the FTC's GLBA privacy rulemaking authority to the Consumer Financial Protection Bureau ("CFPB"), but retained in the FTC (a) GLBA privacy rulemaking authority with respect to automobile dealers and (b) general GLBA privacy enforcement authority over all persons over which the CFPB has jurisdiction for purposes of GLBA privacy rulemaking authority.[3] The CFPB has GLBA privacy rulemaking authority over any person who engages in offering or providing a "consumer financial product or service" as defined by Dodd Frank.[4] Consumer financial products or services are financial products or services that are offered or provided for use by consumers primarily for personal, family or household purposes. Specifically, these products and services are extending credit and loan servicing, extending or brokering leases of personal or real property, real estate settlement services, engaging in deposit taking activities, selling or providing stored value instruments, providing check cashing or check collecting services, providing payments or other financial data

[2] The GLBA originally provided that the Office of Thrift Supervision ("OTS") had GLBA privacy regulatory authority over federally chartered and state-chartered savings banks and savings and loans associations, but the Dodd Frank Act (as defined below) merged portions of the OTS with the OCC, the Federal Reserve, FDIC and the CFPB (as defined below).

[3] See 12 U.S.C. §5512 (the CFPB generally restated existing consumer financial privacy regulations first through a series of interim final rules published in the Federal Register and subsequently through a final rule. 81 FR 25323 (Apr. 28, 2016)).

[4] 12 U.S.C. §5481.

processing services, providing financial advisory services, credit and consumer reporting and debt collection services.[5]

Thus, the CFPB now has GLBA privacy rulemaking authority (but not GLBA security rulemaking authority) for CFPB covered persons providing consumer financial products or services ("Covered Entities"). In addition, the CFPB's GLBA privacy rulemaking jurisdiction includes a "service provider" of a Covered Entity, which is any person that provides a material service to a Covered Entity in connection with the offering or provision by such Covered Entity of a consumer financial product or service ("CFPB Servicer Provider"), subject to certain exceptions, as well as persons engaged in providing a financial product or service within the meaning of the Bank Holding Company Act that do not have a state or another federal functional regulator. Nevertheless, even after Congress passed the Dodd Frank Act, the FTC continues to have GLBA privacy enforcement jurisdiction over financial institutions without a federal or state functional regulator, as well as persons subject to the jurisdiction of the CFPB's GLBA privacy rulemaking authority.

Consistent with Congress' delegation of the regulation of the business of insurance to the states under the federal McCarran-Ferguson Act,[6] the GLBA provides that its privacy and security rules do not affect, alter or supersede any state statute, regulation or order except to the extent inconsistent with the privacy provisions of the GLBA.[7] In response to this reverse preemption, the National Association of Insurance Commissioners ("NAIC") promulgated the NAIC Privacy of Consumer Financial and Health Information Regulation (the "NAIC Privacy Regulation")[8] and the companion NAIC Standards for Safeguarding Customer Information Model Regulation (the "NAIC Security Regulation").[9] Through the adoption of state insurance privacy statutes or regulations embracing the NAIC Privacy Regulation and the NAIC Security Regulation (collectively, the "State Insurance GLBA Privacy Laws"), all states, through their insurance departments, now regulate the collection, use and disclosure of customer[10] nonpublic personal information by entities and individuals engaged in the insurance business.[11]

---

[5] 12 U.S.C. §5481(12)(j).
[6] 15 U.S.C. §§ 1011-1015.
[7] 15 U.S.C. §6824.
[8] NAIC Model Regulation 672-1. Initially promulgated in 2000. The NAIC Privacy Regulation is modeled after the GLBA privacy regulation jointly promulgated by the FDIC, Federal Reserve, FTC, NCUA, OTS and SEC following the passage of the GLBA. The core concepts of the NAIC Privacy Regulation and the FTC's and CFPB's GLBA privacy regulations are the same.
[9] NAIC Model Regulation 673-1.
[10] Claimants under commercial lines policies are also covered by the GLBA.
[11] Approximately 17 states have adopted the NAIC Insurance Information and Privacy Protection Model Act, promulgated by the NAIC in 1982, which preceded the GLBA. These states generally take the position that their adoptions of the NAIC Insurance Information and Privacy Protection Model Act constitute compliance with the GLBA, and enforce them by applying the State Insurance GLBA Privacy Laws.

Locke Lord LLP

Consumer Product Protection Plans and the GLBA

The applicability of State Insurance GLBA Privacy Laws to consumer product protection plans has not been entirely clear since passage of GLBA in 1999 and has become more complex after enactment of the Dodd-Frank Act. Determining whether, and, if so, how, the State Insurance GLBA Privacy Laws apply to these plans, requires an analysis of (i) whether these plans are insurance products or the business of insurance, (ii) if so, whether the McCarran-Ferguson Act reverse preempts the FTC Safeguards Rule, (iii) the applicability of the Magnuson-Moss Warranty Act, which regulates consumer product protection plans at the federal level, and (iv) the post-Dodd-Frank Act division of GLBA privacy and security regulatory jurisdiction between the FTC and the CFPB.

Most states' service contract laws expressly state that extended warranties and home warranties are not insurance. Some have argued that state insurance privacy and security laws implementing the GLBA do not apply to providers of service contracts, even though most such service contract laws grant regulatory and enforcement authority over service contracts to the state insurance regulator. See the Service Contract Industry Council's Position Paper on the Application of Gramm-Leach-Bliley Act to Service Contract Industry, dated July 23, 2001. Therefore, the State Insurance GLBA Privacy Laws adopted in these states arguably do not apply to providers of service contracts, because these GLBA insurance privacy and security laws apply only to products that are not regulated as insurance. In a few states, however, service contracts are not expressly or completely excluded from the applicability of insurance laws, therefore it is more difficult to argue that these contracts are not subject to the State Insurance GLBA Privacy Laws.

A consumer product protection plan, when issued by a third party that is not the manufacturer of the product covered by the plan, is, in most cases, presumptively an insurance contract because it meets the hallmark definition of insurance: risk shifting, risk pooling, indemnity promise, and occurrence of fortuitous event. As a result, most state service contract laws expressly state that service contracts are not insurance. They are, after all, a financial product or service provided to consumers and would be regulated as insurance if not for the statutory exclusion under virtually all states' service contract acts.

The Magnuson-Moss Warranty Act ("MMWA"), which the FTC enforces, also creates some confusion in the area of service contracts. In addition to state service contract laws that define a service contract, the MMWA also defines a service contract as "… a contract in writing to perform, over a fixed period of time or for a specified duration, services relating to the maintenance or repair (or both) of a consumer product." The FTC's MMWA Regulation 700.11(a) recognizes that, in some cases, a service contract can be regulated as insurance under state insurance law.

Under the Dodd-Frank Act, auto dealers, through past effective legislative lobbying efforts, are largely exempt from the supervisory, rulemaking and enforcement authorities of the CFPB, leaving

them usually subject to the FTC's jurisdiction. Generally auto dealers are outside the purview of the CFPB if they regularly sell their auto finance loans or retail installment contracts into the secondary market and do not make to consumers non-automobile loans or provide other consumer financial products and services not regulated by the CFPB. The Dodd-Frank Act also treats a service provider of a covered entity effectively as a CFPB covered entity itself. Subject to certain exceptions, a service provider is a person that provides substantial services to a covered entity, which can include a person that sells a consumer financial product or service not regulated by the CFPB but that is financed by a CFPB regulated lender.[12] Therefore, auto dealers that operate outside of the auto dealer exemption from the definition of covered person, and vehicle service contract ("VSC") obligors that sell their VSCs financed by an auto loan, are likely subject to the GLBA.

GAP Waivers and the GLBA

Most commonly, a GAP waiver is a consumer financial protection product that auto dealers sell to their customers as part of an auto purchase financing package, whereby the lender (often a captive of the auto dealer) will waive its right to collect a portion of the auto loan where the customer's auto insurance policy pays less than the loan balance following a total loss of the auto collateralizing the loan as a result of its damage or theft. Although the legal and regulatory status of these type of GAP waivers was unclear when they were introduced as a novel product, today such GAP waivers are typically treated as an amendment to an auto finance agreement (loan or retail installment contract) and usually considered to be a species of debt-cancellation agreements for the auto finance industry. As such, like service contracts under the laws of most states, such GAP waivers are typically exempted from being classified as insurance, but are nonetheless subject to regulatory oversight in most states by insurance regulators.

Accordingly, GAP waivers issued by lenders other than banks and credit unions are likely subject to the new FTC Safeguards Rule, but whether the FTC or the CFPB has Safeguards Rule enforcement authority depends on the nature of the auto lender. If an auto dealer that is not a Covered Entity is the lender, then the FTC has ranking enforcement authority. On the other hand, a non-auto dealer lender regulated by the CFPB, and a CFPB "service provider" that is the seller of a GAP waiver the purchase price of which is rolled into an auto purchase loan, is subject to the CFPB's enforcement authority for the FTC's new Safeguards Rule. To further complicate matters, where the GAP waiver is issued by a bank or credit union can result in an alternative functional regulator that changes the analysis above.

FTC's vs CFPB's Jurisdiction for GLBA Privacy and Security Regulations

[12] In the context of a vehicle service contract's purchase price that is financed as part of a broader automobile purchase loan, the vehicle service contract obligor become a service provider of the auto purchase loan lender.

Locke Lord LLP

In the post-Dodd Frank Act world, the bifurcation of rulemaking and enforcement authority for the GLBA privacy and security regulations between the FTC and the CFPB breaks down as follows:

Regulatory Agency	GLBA Privacy Rulemaking	GLBA Privacy Enforcement	GLBA Security Rulemaking	GLBA Security Enforcement
CFPB	Regulation P[13] for CFPB Covered Persons and Service Providers	Regulation P for CFPB Covered Persons and Service Providers	None	Via UDAAP[14]
FTC	Auto Dealers and Financial Institutions not CFPB Covered Persons and Service Providers and without other GLBA Functional Regulator	Auto Dealers and Financial Institutions that aren't CFPB Covered Persons and Service Providers and without other GLBA Functional Regulator	Auto Dealers Exempt from CFPB CFPB Covered Persons and Service Providers Financial Institutions not CFPB Covered Persons and Service Providers and without other GLBA Functional Regulator Likely Auto Dealer service contract obligors	Auto Dealers Exempt from CFPB CFPB Covered Persons and Service Providers Financial Institutions not CFPB Covered Persons and Service Providers and without other GLBA Functional Regulator Likely Auto Dealer service contract obligors

[13] 12 CFR Part 1016.
[14] UDAAP means the CFPB's unfair, deceptive, and abusive acts and practices powers. These provides more general enforcement authority.

Locke Lord LLP

State Insurance Cybersecurity Requirements

As referenced above, even though most state service contract laws expressly provide that a service contract is not insurance, many service contract obligors are nonetheless required to be licensed or registered with a state insurance department. The NYDFS Cybersecurity Regulation and the NAIC Data Security Model both apply to businesses that hold licenses or registrations from the state insurance department. Accordingly, for service contract obligors licensed or registered in these states, they are likely subject to both the state insurance cybersecurity laws or regulations as well as the FTC's new Safeguards Rule.

In addition, the NAIC adopted in 2017 its Insurance Data Security Model Law[15], which establishes standards for licensees of state insurance departments for their data security requirements and their obligations to investigate and notify the applicable insurance regulators of cyber security events experienced by such licensees.

Expanded Definition of a Financial Institution under the new FTC Safeguards Rule

The FTC's GLBA privacy and security regulations broadly define financial institution. The GLBA "applies to businesses that are 'significantly engaged' in 'financial activities' as described in section 4(k) of the Bank Holding Company Act."[16] According to the Bank Holding Company Act provision and regulations established by the Federal Reserve Board, "financial activities" include the following activities.

- Lending, exchanging, transferring, investing for others, or safeguarding money or securities. These activities cover services offered by lenders, check cashers, wire transfer services, and sellers of money orders.
- Providing financial, investment or economic advisory services. These activities cover services offered by credit counselors, financial planners, tax preparers, accountants, and investment advisors.
- Brokering loans.
- Servicing loans.
- Debt collecting.
- Providing real estate settlement services.

[15] NAIC Model Law 668.
[16] 12 U.S.C. 1843(k)(4).

- Career counseling (of individuals seeking employment in the financial services industry).

In addition, the recently proposed changes to the FTC Safeguards Rule will add to the definition of a financial institution, and expand it to include, any "institution that is significantly engaged in financial activities, or *significantly engaged in activities incidental to such financial activities* ...."[17] This new category of activities considered to be "incidental to financial activities" is specifically enumerated under the FTC's proposed regulation and currently only includes a "finder," which means "bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate."[18] To expand on this description of a finder, the proposed regulation describes the scope of finder activities as follows:

> "**(i)** ***What is the scope of finder activities?*** Acting as a finder [, such as customer lead generators for consumer financial products or services,] includes providing any or all of the following services through any means -
>
> **(A)** Identifying potential parties, making inquiries as to interest, introducing and referring potential parties to each other, and arranging contacts between and meetings of interested parties;
>
> **(B)** Conveying between interested parties expressions of interest, bids, offers, orders and confirmations relating to a transaction; and
>
> **(C)** Transmitting information concerning products and services to potential parties in connection with the activities described in paragraphs (d)(1)(i)(A) and (B) of this section."[19]

To the extent that a company is regulated by the FTC, financial institutions would include auto dealers that lease autos in the ordinary course of business, and may also include companies offering service contracts to the extent they are not regulated as the business of insurance. Therefore, because a service contract is likely provided to consumers by financial institutions, the FTC's GLBA regulations, including the new FTC Safeguards Rule, should apply to service contracts.

Previous Safeguards Rule

The old Safeguards Rule was simple in contrast to the new rule. For background, the FTC has promulgated two rules to implement the GLBA: the Privacy Rule and the Safeguards (or security) Rule. The Privacy Rule restricts the disclosure of consumer's nonpublic personal information and requires financial institutions to provide consumers with various notice and opt-out rights with regards to the collection and disclosure of their GLBA protected information. The Safeguards Rule is a set of administrative, technical, and physical security requirements that must be applied

[17] 16 CFR part 314.2(f) (emphasis added).
[18] 12 CFR 225.86(d)(1).
[19] See 12 CFR § 225.86(d)(1)(i).

to GLBA protected information in order to secure that information against unauthorized access, acquisition, or disclosure. Before the recent update, the Safeguards Rule was flexible and kept its requirements general. The old FTC Safeguards Rule required a Y2K "1.0" version of data security, that financial institutions implement an information security program that included: performing risk assessments, implementing safeguards to control and monitor against the identified risks, overseeing service providers, and providing ongoing updates to the program as material changes occur to ongoing business risks.

Implemented New Changes (effective December 2022)

The new FTC Safeguards Rule ushers in a set of rules similar to those in the NYDFS Cybersecurity Regulation. These new requirements include the following:

- Designation of a "CISO" type individual who is responsible for the information security program and must regularly report to the board of directors (or equivalent);
- Push down of additional information security program requirements to service providers or affiliates;
- New oversight obligations including regular audits of those service providers;
- Additional criteria when performing the required risk assessments, such as performing data and device inventories;
- Data protection, such as requiring encryption for customer data in transit and at rest, with certain limited exceptions;
- Secure development practices;
- Implementation of multi-factor authentication;
- Secure disposal practices;
- Additional monitoring and logging practices, in addition to change management practices;
- Performance of vulnerability and penetration testing, or continuous security monitoring;
- Written incident response plan; and
- Documentation of these updates with additional policies.

Notably these requirements are partially limited for smaller companies. If the regulated company maintains "customer information" of fewer than 5,000 consumers, the company will be permitted to: (i) perform a more limited risk assessment; (ii) avoid the mandatory continuous monitoring and penetration testing requirements; (iii) avoid maintaining a separate written incident response plan; and (iv) avoid requiring the CISO to regularly report to the board of directors (or equivalent).

Locke Lord LLP

In total, these new requirements will be a dramatic change for entities currently subject to FTC's GLBA jurisdiction and a more important diligence matter for private equity firms that invest in service contract providers and administrators. In addition, to the extent that they are not already subject to the requirements of the NYDFS Cybersecurity Regulation, the new FTC Safeguards Rule imposes new obligations on insurance companies that have service contracts administrative agreements with service contract providers and that insure their products through contractual liability insurance policies as required under state service contract provider licensing laws.

More Amendments on the Horizon

In addition to these updates to the Safeguards Rule, the FTC has proposed further rulemaking () that would add notice obligations following a security incident that meets certain thresholds. The FTC will require notice on a web-portal, within 30 days of discovery of the incident, if a regulated entity determines "that misuse of customer information has occurred or is reasonably likely and that at least 1,000 consumers have been affected or reasonably may be affected[.]" The electronic notice must include (i) the name and contact information of the reporting financial institution; (ii) a description of the types of information that were involved in the security event; (iii) if the information is possible to determine, the date or date range of the security event; and (iv) a general description of the security event.

If this further rulemaking goes into effect, it would represent a major shift in the direction of notice obligations for regulated entities, many of which have been subject only to state security incident notice obligations.

What's next?

Service contract providers, auto dealers, and many other FTC regulated entities will soon be required to implement and maintain enhanced safeguards to protect the customer data they maintain, on parity with financial companies subject to the NYDFS Cybersecurity Regulation. While these obligations are burdensome for many regulated companies, they also represent important investments in information security that will provide benefits, such as reducing the company's exposure to the continuing threat of ransomware and other cybersecurity attacks.

We recommend taking a step by step process to compliance and starting as soon as possible. While these new requirements are extensive, they only apply to consumer information that is collected subject to the GLBA. As such, it will be important for regulated companies to begin taking steps as soon as possible to prepare for the December 2022 compliance deadline.

Locke Lord LLP

Brian T. Casey
Partner
Atlanta
404-870-4638
bcasey@lockelord.com

Brian T. Casey is Co-Leader of Locke Lord's Regulatory and Transactional Insurance Practice Group, and a member of the Firm's Corporate, Capital Markets and Health Care Practice Groups. Brian focuses on corporate, merger and acquisition, corporate and structured finance, and other transactional and regulatory matters for corporate clients in the insurance, financial services and health care industries. His clients include insurance companies, insurance holding companies, managing general agents and insurance agencies, third party and claims administrators, banks and other financial institutions, investment banks and reinsurance companies.

Theodore P. Augustinos
Partner
Hartford
860-541-7710
ted.augustinos@lockelord.com

Ted Augustinos advises clients in various industries on privacy and data protection, cybersecurity compliance and incident preparedness, and breach response. He is a member of the Steering Committee of the Firm's Privacy and Cybersecurity Practice Group, and leads the group's initiatives focused on the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA), and New York DFS Cybersecurity Regulation, and its Incident Response Team. He is a Certified Information Privacy Professional, accredited by the International Association of Privacy Professionals. Ted serves as Co-Chair of the World Law Group's Data Protection and Privacy Group, and as Managing Partner of the Hartford, Connecticut office of Locke Lord.

Alexander R. Cox
Associate
Hartford
860-541-7756
alex.cox@lockelord.com

Alex Cox advises clients in various industries on privacy and cybersecurity issues, from implementing information security and incident response programs to addressing compliance questions and providing guidance in a variety of contexts, for clients ranging from startups to large, highly regulated organizations.

Alex is the Chair of the Executive Committee of the Connecticut Bar Association's Young Lawyers Section on Cybersecurity and Technology and is a CIPP/US Certified Privacy Professional. His technical data analytics background informs his advice to clients.