Customer Privacy Protection under the Gramm-Leach-Bliley Act

Introduction: Why Do We Need Customer Data Disclosure Protections?

Most people are reluctant to discuss with strangers those parts of their lives they consider personal. The address where you live, what your income is, how much you owe others, and information like your Social Security number or driver's license number are all things you guard carefully. It is reasonable to expect that when you must give such personal information to others, like to a mortgage broker when applying for a mortgage loan, that they will safeguard it, too.

Balanced against this reasonable expectation of personal information privacy is the reality that not everyone else will voluntarily protect the data you give them with the same care you would. People can be careless in how they safeguard your information. Some of them may be willing to share it with others who want access to it and, indirectly at least, to you. And they can do it all behind your back: as one former Commissioner of the Federal Trade Commission (FTC) put it,

> *"Today, personal information about an individual is being collected at a rate and to a degree unthinkable even five years ago. Currently, much of an individual's personal information can be legally collected, shared, exchanged, sold, and disseminated without notice to or input by the individual."*[1]

Today's consumer can become confused and concerned about what a company does with that person's data. For example, according to a 2019 survey on data privacy, most survey participants believed that companies exercise little or no control over the data they collect.[2] Majorities stated that they are uneasy about how companies collect their data, that they have little understanding of what companies do with their data, and that the potential risks of companies collecting their data outweigh the benefits of their doing so.[3]

The federal government and a growing number of state governments have enacted laws to require companies that collect customer data to notify customers of the fact and to give them the option to decline to have their data shared with outsiders. In this course we focus on one federal data privacy protection law, the Gramm-Leach-Bliley Act (GLB Act),[4] with emphasis on its disclosure requirements to mortgage loan consumers and customers.

Purpose and Structure of the GLB Act

The purposes of the GLB Act are to restrict how financial institutions disclose certain consumer and customer information to nonaffiliated third parties, to require companies to have information security plans to protect customer data from unauthorized access, and to make illegal unauthorized attempts to access customer data. Multiple federal agencies enforce the GLB Act through regulations. For example,

---

[1] Consumer Privacy in the Information Age: A View from the United States | Federal Trade Commission (ftc.gov)
[2] Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information | Pew Research Center
[3] Id.
[4] https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm

the FTC states the requirements for information security plans in its Safeguarding Rule.[5] For mortgage brokers and lenders, and for the limited purposes of this course, we will confine our examination of GLB Act enforcement to how the Consumer Financial Protection Bureau (CFPB) requires companies to issue initial, revised, and annual privacy notices to consumers and customers under rules collectively known as "Regulation P."[6]

Mortgage Companies as Financial Institutions Under the GLB Act

Before we go into the details of how Regulation P works, first we will establish how the CFPB has authority over mortgage lenders and brokers under the GLB Act.

Regulation P applies to financial institutions.[7] Under Regulation P, an institution that is significantly engaged in financial activities is a financial institution.[8] A financial institution includes a provider of real estate settlement services.[9] Under the Real Estate Settlement Procedures Act, settlement services include taking loan applications, underwriting, and funding of loans.[10] In addition, Regulation a P specifically includes mortgage broker as a financial institution.[11]

Distinguish Regulation P from the FTC Financial Privacy Rule

The FTC has a disclosure rule that is identical to Regulation P, the Financial Privacy Rule.[12] Although the Financial Privacy Rule reads identically to Regulation P, including references to mortgage brokering,[13] it is mostly limited in its application to automobile dealerships and as a matter of policy the FTC does not apply it to mortgage companies.[14]

How Regulation P Protects Consumer and Customer Data Privacy

Fundamentally, Regulation P prohibits you and your affiliates from disclosing consumer or customer NPI to a nonaffiliated third party unless:[15]

- You have provided an initial privacy notice
- You have given notice of the right to opt out
- You have given a reasonable opportunity to opt out before making a disclosure of NPI, and the consumer or customer does not opt out.

---

[5] Document (ftc.gov)
[6] 12 CFR Part 1016 - Privacy of Consumer Financial Information (Regulation P) | Consumer Financial Protection Bureau (consumerfinance.gov)
[7] 12 CFR 1016.1(b)(1)
[8] 12 CFR 1016.3(l)(3)(i)
[9] 12 CFR 1016.3(l)(3)(ii)(J)
[10] 12 U.S.C. 2602(3)
[11] 12 CFR 1016.3(l)(3)(ii)(K)
[12] eCFR :: 16 CFR Part 313 -- Privacy of Consumer Financial Information
[13] See 16 CFR 313.3(i)(2)(i)(D) and 16 CFR 315.5(b)(2)(ii)
[14] https://www.federalregister.gov/d/2021-25735/p-54 at footnote 31: The FTC *"…continues to believe that mortgage loans are unlikely to be involved in the motor vehicle dealer context."* The FTC has left mortgage brokering references in the Financial Privacy Rule because *"…there is value in maintaining consistency with Regulation P, and that particular examples provided may not be applicable to every type of financial institution's activities. Accordingly, the final rule retains the references to mortgage loans in these provisions."*
[15] 12 CFR 1016.8(a)

Not all consumer and customer data is subject to protection by companies that collect such data. To identify information subject to disclosure notices, we must determine to whom NPI might be disclosed, whether the information is publicly available information or non-public personal information (NPI), and whether the individual whose NPI is subject to disclosure is a consumer or a customer.

Third Parties Versus Nonaffiliated Third Parties

Even if information subject to disclosure is NPI, you do not need to provide a privacy notice to consumers or customers if the persons you disclose it to are affiliated with you. Regulation P only requires privacy notice disclosures when you reveal NPI to nonaffiliated third parties.[16] Under Regulation P, a nonaffiliated third party is anyone who is not an affiliate of yours[17] or someone you employ jointly with another company.[18] An affiliate includes a company that you control, or that you share control over with another company.[19]

Is the Information Publicly Available?

Companies have no obligation to safeguard publicly available information. Publicly available information is information that you reasonably believe is lawfully made available to the public.[20] A reasonable basis to believe that information is publicly available can be steps you take determine that the information is public,[21] or whether a person can direct that the information not be made public and does not do so.[22]

Information found in federal, state, and local government records, like mortgage information in real estate records,[23] [24] can be considered publicly available.[25] Other examples are information gained from widely distributed media[26] like a newspaper, television or radio program, or public telephone directory,[27] or public disclosures that are required under federal, state, or local law.[28]

Nonpublic Personal Information

NPI is information includes personally identifiable financial information[29] and any list, description, or other grouping of consumers put together with information not publicly available.[30] Examples of lists using nonpublic personal information include lists of the names and addresses of people you derive from personally identifiable information, like account numbers.[31]

---

[16] 12 CFR 1016.8(a)
[17] 12 CFR 1016.3(o)(1)(i)
[18] 12 CFR 1016.3(o)(1)(ii)
[19] 12 CFR 1016.3(a)(1)
[20] 12 CFR 1016.3(r)(1)
[21] 12 CFR 1016.3(r)(2)(i)
[22] 12 CFR 1016.3(r)(2)(ii)
[23] 12 CFR 1016.3(r)(3)(i)
[24] 12 CFR 1016.3(r)(3)(iii)(A)
[25] 12 CFR 1016.3(r)(1)(i)
[26] 12 CFR 1016.3(r)(1)(ii)
[27] 12 CFR 1016.3(r)(3)(ii)
[28] 12 CFR 1016.3(r)(1)(iii)
[29] 12 CFR 1016.3(p)(1)(i)
[30] 12 CFR 1016.3(p)(2)(ii)
[31] 12 CFR 1016.3(p)(3)(i)

Personally Identifiable Financial Information

Personally identifiable financial information (PIFI) is information a consumer gives you in exchange for a financial product or service you provide,[32] such as information on a loan application.[33] PIFI also includes consumer information that comes from a financial product or service transaction between you and a customer,[34] and information you obtain about a customer in connection with providing that financial product or service.[35] Information such as lists of customers of a company that is not a financial institution is not PIFI.[36] Nor is information that does not identify the consumer or contain information types that Regulation P identifies as PIFI.[37]

Aside from personal addresses and account numbers mentioned above, other kinds of PIFI under Regulation P include account balance information, payment and overdraft histories, credit or debit card purchase information, [38] the existence of a current or past customer relationship with you,[39] information that identifies the individual as a consumer of yours,[40] information you receive from a consumer in connection with loan servicing or collections,[41] information from consumer reports,[42] and online tracking information you obtain from Internet "cookies."[43]

Customers or Consumers?

Consumers and customers share the commonality that all customers are consumers. Not all consumers, however, become customers.

Consumers

A consumer is an individual who obtains or who has obtained a financial product or service for primarily personal, family, or household use.[44] If applying for a loan, it is not necessary for the loan to be approved for consumer status to apply.[45]

Customers

The difference between a consumer and a customer is that a customer has a continuing relationship with you.[46] For mortgage lenders and brokers, a continuing relationship is one in which a consumer obtains a loan with you[47] or enters into an agreement with you in which you provide home mortgage brokering services.[48]

---

[32] 12 CFR 1016.3(q)(1)(i)
[33] 12 CFR 1016.3(q)(2)(i)(A)
[34] 12 CFR 1016.3(q)(1)(ii)
[35] 12 CFR 1016.3(q)(1)(iii)
[36] 12 CFR 1016.3(q)(2)(ii)(A)
[37] 12 CFR 1016.3(q)(2)(ii)(B)
[38] 12 CFR 1016.3(q)(2)(i)(B)
[39] 12 CFR 1016.3(q)(2)(i)(C)
[40] 12 CFR 1016.3(q)(2)(i)(D)
[41] 12 CFR 1016.3(q)(2)(i)(E)
[42] 12 CFR 1016.3(q)(2)(i)(G)
[43] 12 CFR 1016.3(q)(2)(i)(F)
[44] 12 CFR 1016.3(e)(1)
[45] 12 CFR 1016.3(e)(2)(ii)
[46] 12 CFR 1016.3(i)
[47] 12 CFR 1016.3(j)(2)(i)(B)
[48] 12 CFR 1016.3(j)(2)(i)(F)

Note that who owns a mortgage loan and who services the loan makes a difference in establishing a customer relationship. The party that services the loan has the customer relationship with the homeowner.[49] If you sell a mortgage loan to another loan servicer and do not retain servicing rights, then the homeowner becomes that company's customer and becomes a past customer and a consumer of yours.[50]

Mortgage Company Obligations to Consumers and Customers Under Regulation P

Initial Privacy Notices to Consumers

Usually, if you have a consumer relationship with an individual, then before you disclose any NPI about that person then that individual is entitled to receive an initial privacy notice from you.[51] You must give this notice to the consumer before you make a disclosure of that person's NPI to a nonaffiliated third party.[52]

Exceptions to Consumer Initial Notice Requirements

You do not need to give an initial privacy notice to a consumer if you do not disclose NPI to nonaffiliated third parties[53] and you do not have any other customer relationship with that person.[54] Also, Regulation P recognizes other exceptions to the initial consumer privacy notice requirement. These include when you disclose NPI to:

- comply with the direction of the consumer or with the consumer's consent, so long as the consumer does not revoke the direction or consent[55]
- protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liabilities[56]
- resolve consumer disputes or inquiries, or for institutional risk control purposes[57]
- protect the confidentiality or security of your records related to the consumer, the financial product or service, or the transaction with the consumer[58]
- you disclose NPI as needed to implement, administer, or enforce a transaction at the request or authorization of the consumer[59]
- service or process a financial product or service the consumer requests or authorizes[60]

---

[49] 12 CFR 1016.3(j)(2)(i)(C)
[50] 12 CFR 1016.3(j)(2)(ii)(B)
[51] 12 CFR 1016.4(a)(2)
[52] Id.
[53] 12 CFR 1016.4(b)(1)
[54] 12 CFR 1016.4(b)(2)
[55] 12 CFR 1016.15(a)(1)
[56] 12 CFR 1016.15(a)(2)(ii)
[57] 12 CFR 1016.15(a)(2)(iii)
[58] 12 CFR 1016.15(a)(2)(i)
[59] 12 CFR 1016.14(a)
[60] 12 CFR 1016.14(a)(1)

- disclose NPI to persons who have a legal or beneficial interest related to the consumer,[61] or to persons who are legal representatives or fiduciaries of the consumer[62]
- disclose NPI involving the sale or proposed sale of servicing rights to a financial product or service[63]
- provide information needed by agencies that evaluate your compliance with industry standards, and to your own accountants, auditors, and lawyers[64]
- comply with federal, state, or local laws or rules,[65] or with a properly authorized criminal, regulatory, or civil investigation, or with a federal, state, or local subpoena or summons[66] or to reply to regulatory or judicial authorities that have jurisdiction over you for compliance, examinations, or other lawful purposes[67]
- disclose NPI to law enforcement agencies, or to self-regulatory organizations, or in connection with a public safety-related investigation or matter[68]
- disclose NPI to a consumer reporting agency under the Fair Credit Reporting Act,[69] or disclose NPI received from such an agency[70]

Initial Privacy Notices to Customers

You must provide a required initial notice to a customer when you enter a customer relationship[71] or within a reasonable time after the customer relationship begins if the creation of the customer relationship happens without the election of the customer[72] or if waiting to provide the notice would substantially delay the customer transaction and the customer agrees to receive the initial notice later.[73] For financial institutions, the customer relationship begins when the loan originates or when an institution purchases the servicing rights to the loan.[74]

Revised Privacy Notices to Current Customers

For an existing customer who obtains a new financial product or service, you can provide a revised privacy notice.[75] [76] Or, if the most recent annual or revised privacy notice sent to the customer accurately covers the new product or service, then no new privacy notice is required.[77]

---

[61] 12 CFR 1016.15(a)(2)(iv)
[62] 12 CFR 1016.15(a)(2)(v)
[63] 12 CFR 1016.14(a)(3)
[64] 12 CFR 1016.15(a)(3)
[65] 12 CFR 1016.15(a)(7)(i)
[66] 12 CFR 1016.15(a)(7)(ii)
[67] 12 CFR 1016.15(a)(7)(iii)
[68] 12 CFR 1016.15(a)(4)
[69] https://www.govinfo.gov/link/uscode/15/1681
[70] 12 CFR 1016.15(a)(5)
[71] 12 CFR 1016.4(c)(1)
[72] 12 CFR 1016.4(e)(2)(i)
[73] 12 CFR 1016.4(e)(2)(ii)
[74] 12 CFR 1016.4(e)(2)(i)(A)
[75] 12 CFR 1016.4(d)(1)
[76] eCFR :: 12 CFR 1016.8 -- Revised privacy notices
[77] 12 CFR 1016.4(d)(2)

Annual Privacy Notices to Customers

Unless an exception applies you must give a renewal privacy notice to your customers every 12 months. You may decide what the 12-month period is, so long as you apply it consistently to the customer.[78]

Exceptions to the annual privacy notice requirement include when you only provide NPI to unaffiliated third parties under a recognized exception like a customer-requested transaction or to comply with government-required disclosures,[79] or if you have not changed your privacy policies and procedures since the most recent privacy notice given to the customer.[80] If you make any changes, however, then depending on what notice if any the customer already had you will either need to give the customer a revised privacy notice within 100 days of the policy change[81] or, if you were not giving notices to the customer under an exception, then you will need to give the customer an initial privacy notice.[82]

What Goes into a Proper Privacy Notice?

Regulation P lays out the requirements for initial, renewal, and annual privacy notices to be valid.

- They must be clear and conspicuous. This means that the notice must be reasonably understandable and designed to call attention to the nature and significance of the notice.[83]
    - Notices that use concise sentences, paragraphs, and sections, and which are written in active voice and using everyday vocabulary words, are examples of being reasonably understandable.[84]
    - Notices designed to call attention to their content use easy-to-read text with plain-language headings and bold face or Italic text for key terms or provisions.[85]
    - Regulation P also has clarity and conciseness guidance for companies that provide online privacy notices, to ensure that readers can view the entire notice in a place where the reader is likely to see it and not be distracted by other elements on the web page.[86]
- They must state the kinds of NPI you collect[87] and the kinds of NPI you disclose.[88] This includes NPI obtained from a consumer reporting agency or disclosure of information like names, addresses, phone numbers, and account balances.
- They must state the kinds of affiliates and nonaffiliated third parties you disclose NPI to, other than those that would qualify you for an exception to the notice requirement.[89] This information can include financial services providers, insurance companies, mortgage brokers, nonprofit organizations, and direct marketers.

---

[78] 12 CFR 1016.5(a)(1)
[79] 12 CFR 1016.5(e)(1)(i)
[80] 12 CFR 1016.5(e)(1)(ii)
[81] 12 CFR 1016.5(e)(2)(ii)
[82] 12 CFR 1016.5(e)(2)(ii)
[83] 12 CFR 1016.3(b)(1)
[84] 12 CFR 1016.3(b)(2)(i)
[85] 12 CFR 1016.3(b)(2)(ii)
[86] 12 CFR 1016.3(b)(2)(iii)
[87] 12 CFR 1016.6(a)(1)
[88] 12 CFR 1016.6(a)(2)
[89] 12 CFR 1016.6(a)(3)

    - If you disclose NPI to a nonaffiliated third party under a recognized exception, then you must provide a separate statement of the kinds of information you disclose and the kinds of third parties to whom you are making the disclosures to.[90]
- They must explain the consumer or customer's right to opt out of the disclosure of NPI, including how the consumer or customer can reasonably exercise that right.[91] Partial opt-outs, in which the consumer or customer can select which nonaffiliated third parties may receive NPI, are acceptable.[92]
    - A reasonable means to opt out can include a toll-free telephone number,[93] or a detachable form with a check-off box and mailing information.[94]
    - A procedure that requires a customer or consumer to write a letter to opt out, without any other option, is not a reasonable means.[95]
    - Customers and consumers can exercise their opt-out rights at any time.[96] It is your responsibility to comply with an opt-out request as soon as you reasonably can.[97]
    - An opt-out request is effective until the customer or consumer cancels it in writing, or electronically if the customer agrees to that means.[98]
    - If a former customer enters a new transaction with you, then you must provide the customer with a new opt-out notice that applies only to the new transaction.[99]
- They must identify disclosures you make to affiliates under the Fair Credit Reporting Act and give opportunity for the customer to opt out of such disclosures.[100]
- They must state your policies and practices to protect the confidentiality and security of NPI.[101] These must include a general description of who is authorized to access NPI[102] and state whether you have security practices and procedures in place to ensure confidentiality of information in accordance with your policy.[103]
    - Although it is not necessary to describe your policies and practices in technical detail,[104] if you have them in place then you must make a genuine effort to implement and enforce them.
    - Note that although it does not ordinarily apply the Financial Privacy Rule to mortgage lenders or brokers, the FTC can act if the failure to provide a clear and conspicuous notice to customers rises to the level of false or misleading statements.[105] [106]

---

[90] 12 CFR 1016.6(a)(5)
[91] 12 CFR 1016.6(a)(6)
[92] 12 CFR 1016.10(c)
[93] 12 CFR 1016.7(a)(2)(ii)(D)
[94] 12 CFR 1016.10(a)(3)(i)
[95] 12 CFR 1016.7(a)(2)(iii)(A)
[96] 12 CFR 1016.7(h)
[97] 12 CFR 1016.7(g)
[98] 12 CFR 1016.7(a)(2)(ii)(C)
[99] 12 CFR 1016.7(i)(2)
[100] 12 CFR 1016.6(a)(7)
[101] 12 CFR 1016.6(a)(8)
[102] 12 CFR 1016.6(c)(6)(i)
[103] 12 CFR 1016.6(c)(6)(ii)
[104] Id.
[105] Mortgage Company Settles Data Security Charges | Federal Trade Commission (ftc.gov)
[106] Complaint (ftc.gov)

- They must identify disclosures you make to nonaffiliated third parties who are subject to exceptions.[107] If you disclose NPI under an exception to the notice requirements, then although you are not required to identify the parties you can state that you make disclosures to other nonaffiliated companies for everyday business purposes, like processing transactions, maintaining accounts, responding to court orders or legal investigations, or to reporting to credit bureaus.[108]

The Model Privacy Form

Regulation P includes a Model Privacy Form.[109] Financial institutions that use the model form as a safe harbor to show compliance with Regulation P disclosure requirements, so long as they make no changes to it or add information except where the form instructions permit.[110]

Privacy Notice Delivery to Consumers and Customers

The purpose of the Regulation P notice delivery rule is to guide financial institutions on delivery means they can use to have a reasonable expectation of actual notice.[111]

- Unless the consumer or customer agrees to electronic delivery, privacy notices, including short-form notices, must be given to the consumer or customer in writing.[112]
- Oral notice delivery, such as explaining the notice to the consumer or customer over the telephone or in person, is insufficient.[113]
- Reasonable delivery means include hand delivery[114] or mailing to the individual's last known address.[115]

If the consumer or customer has agreed to electronic notice, then the notice posted on the website should be clearly and conspicuously visible and require the consumer or customer to acknowledge receipt of the notice as a prerequisite to obtaining a financial product or service.[116]

Examples of notice delivery that do not provide reasonable expectation of actual notice include only posting a sign in your office or at a branch location, or in published advertisements.[117] If your customer has not obtained a financial product or service from you electronically, then electronic notice delivery is also an unreasonable way to expect your customer has received actual notice.[118]

---

[107] 12 CFR 1016.6(a)(9)
[108] 12 CFR 1016.6(c)(2)(ii)
[109] Appendix to Part 1016 - Model Privacy Form | Consumer Financial Protection Bureau (consumerfinance.gov)
[110] 12 CFR Appendix to Part 1016 B.1.(b)
[111] 12 CFR 1016.9(b)(1)
[112] 12 CFR 1016.9(a)
[113] 12 CFR 1016.9(d)
[114] 12 CFR 1016.9(b)(1)(i)
[115] 12 CFR 1016.9(b)(1)(ii)
[116] 12 CFR 1016.9(b)(1)(iii)(A)
[117] 12 CFR 1016.9(b)(2)(i)
[118] 12 CFR 1016.9(b)(2)(ii)

Penalties for GLB Act Violations

The FTC[119] and the CFPB[120] have authority to enforce the GLB Act against violations of its provisions. The FTC or the CFPB can bring actions to enforce the GLB Act in federal district court to seek injunctive and equitable relief. Company civil penalties for violations can be up to $100,000 per violation, and officers and directors of the company can be personally liable for up to $10,000 for each violation.[121] The company and its directors and officers can also be subject to fines and imprisonment for up to five years under Title 18 of the U.S. Code.[122]

An example of privacy notice enforcement, although not directly related to Regulation P, is how the FTC applied the identical Financial Privacy Rule to a financial institution that provided its privacy notices online. The FTC accused the company of failing to make its notice clear and conspicuous because the notice did not call attention to the nature and significance of the notice. Specifically, the privacy notice text was colored grey and set against a light grey background; the notice contained inaccuracies about who the institution shared information with; and the privacy notice did not require customers to acknowledge receipt.[123] In the settlement agreement with the FTC, the accused financial institution did not have to pay any monetary penalties, but in addition to corrective actions it was also subject to biennial assessments, compliance monitoring and reports, and additional recordkeeping requirements for 20 years. The financial institution was also permanently enjoined from further violations of Regulation P or the Financial Privacy Rule.[124]

State Data Privacy Protection Laws

The GLB Act allows for state laws to protect consumer and customer data privacy if those laws are not inconsistent with the GLB Act.[125] A state law that provides more consumer and customer protections than the GLB act is consistent with the GLB Act.[126]

Conclusion

Because of the existence of specifically identified regulatory requirements for valid privacy notices, along with CFPB guidance to interpret those requirements, Regulation P privacy notice violations are not an area of high frequency enforcement by the CFPB. The existence of model forms that can provide safe harbor when used properly also helps to reduce the frequency of violations. Perhaps the most important thing for mortgage brokers, lenders, and servicers about Regulation P and the GLB Act is that the model forms alone are not enough to avoid privacy notice violations if the information that goes into them is not accurate or if delivery to the consumer does not meet the expectation of actual delivery requirements. Also, sound practice should include investigation of state consumer privacy laws, because these can have requirements in addition to those found in Regulation P.

---

[119] How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act | Federal Trade Commission (ftc.gov)
[120] 12 USC Sections 5481(12)(J), 5514(b)-(c), and 5515(b)-(c)
[121] https://www.govinfo.gov/content/pkg/BILLS-107s450is/html/BILLS-107s450is.htm
[122] 18 U.S. Code § 3551 - Authorized sentences | U.S. Code | US Law | LII / Legal Information Institute (cornell.edu)
[123] PayPal Settles FTC Charges that Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act | Federal Trade Commission
[124] Id.
[125] 15 USC 6807: Relation to State laws (house.gov)
[126] Id.

Quiz

1. Which of the following is true about the relationship between the FTC Financial Privacy Rule and Regulation P?
    a. Regulation P is limited mostly to loans made by automobile dealers.
    b. The FTC is the agency responsible for enforcing Regulation P.
    c. Regulation P and the Financial Privacy Rule are identical in their privacy notice requirements.
    d. Remedies and penalties for violations of the Financial Privacy Rule and Regulation P are different from one another.
    Answer: C

2. Which of the following is not a prerequisite to disclosure of NPI to nonaffiliated third parties?
    a. You must provide an initial privacy notice.
    b. You must have already provided the financial product or service to the consumer or customer before the notice is required.
    c. You must give the consumer or customer a right to opt out of NPI disclosures.
    d. The customer or consumer must not have exercised any opt-out option.
    Answer: B

3. Which of the following best describes the difference between a consumer and a customer?
    a. All consumers are customers.
    b. All customers are consumers.
    c. Consumers are entitled under Regulation P to receive annual renewal privacy notices.
    d. Consumers are not covered by privacy notice requirements, only customers are.
    Answer: B

4. Which of the following is not a source of personally identifiable financial information?
    a. Information on a loan application.
    b. Information that comes from a customer transaction.
    c. Information you obtain about a customer when providing a financial product or service.
    d. Information obtained from government public records.
    Answer: D

5. Disclosing NPI to a law enforcement agency in connection with an investigation is best described as:
    a. An exception to the requirement to provide an initial consumer privacy notice.
    b. Prohibited by Regulation P unless the consumer or customer consents.
    c. Prohibited by Regulation P if the customer has opted out of disclosures to nonaffiliated third parties.
    d. An example of publicly available information.
    Answer: A

6. Which of the following is not true about annual privacy notices?
    a. They are based on the calendar year.
    b. If you have not changed your privacy policies and procedures since the last notice given to the customer, then you do not need to provide a new annual notice.
    c. Annual notices are not required for consumers.
    d. Annual notices are not required if you only disclose NPI to unaffiliated third parties under a recognized regulatory exception to the privacy notice requirement.
    Answer: B

7. Which of the following is true about the relationship between the GLB Act and state consumer privacy laws?
    a. The GLB Act supersedes state consumer privacy laws.
    b. State consumer privacy laws are allowable, but they must mirror the provisions of the GLB Act's privacy notice requirements.
    c. States have rulemaking and enforcement authority to implement Regulation P.
    d. State laws can provide consumer privacy protections beyond those provided for in the GLB Act.
    Answer: D

8. Which of the following is not true about a consumer or customer's opt-out rights to NPI disclosures?
    a. A toll-free telephone number to call is a reasonable means for a customer or consumer to opt out.
    b. Customers and consumers can exercise their opt-out rights at any time.
    c. An opt-out election is only valid until the next time the consumer or customer receives a revised or annual privacy notice.
    d. If a former customer enters a new transaction with you, then you must give the customer a new opt-out notice related to the new transaction.
    Answer: C

9. Which of the following would be the least likely to be considered "clear and conspicuous" notice under Regulation P?
    a. Plain-language headings and easy-to-read text.
    b. Use of everyday vocabulary and active voice.
    c. Bold face or Italic type for important terms or provisions.
    d. Notice written in small text on a background that reduces the contrast with the text.
    Answer: D

10. Which of the following is not true about online privacy notices?
    a. Online notices are only allowed in addition to written copies of notices that the customer or consumer has actually received.
    b. Online notices should be placed on the web page so that other page elements do not distract from them.
    c. Online notices must be acknowledged by the consumer or customer.
    d. Online notices must be in a place on the web page where consumers or customers are likely to see them.

    Answer: A