Customer Data Privacy and Information Security for Mortgage Professionals

For better and for worse, one effect of advancing electronic technology is that it has radically expanded the reach of people and companies. A positive example is the growth of the online marketplace for goods and services: having a website that can serve customers anywhere in the world is standard practice even for small businesses today.

A negative example is the growing problem of cyber criminals. Before the Internet, the harm a burglar, pickpocket, embezzler, or con artist could do was largely confined to that person's physical reach. Today cybercrime is as global as the Internet that gave birth to it. Your customers and your would-be victimizers can both reach you from almost anywhere through a variety of devices and communications networks.

For mortgage professionals the integration of the Internet into their operations is that they now have opportunities and face risks that did not exist in significant form as recently as the 1990s. It is not hyperbole to say that modern electronic financial technology – colloquially known as "FinTech" – has revolutionized the way the American mortgage lending industry does business. The old model of physical branches staffed by brokers, in-person interactions with consumers and customers, paper-based recordkeeping is being supplemented by online mortgage applications, centralized operations, and automated underwriting procedures. In 2022, for example, an online company that offered loan approvals in as little as eight minutes was the largest mortgage lender in the United States.[1]

The purpose of this course is to familiarize you with the information security environment that mortgage lenders operate in. Specifically, we identify the kinds of information you need to safeguard, cover threats to information security, introduce you to relevant government cybersecurity laws and regulations that apply to mortgage lenders, and to provide some best practices and resources to use in your information security program.

What is Consumer or Customer Data?

The starting point to understanding the importance of information security is to know the kinds of customer data that you must protect. This depends in part on whether you deal with consumers or customers, and the nature of the information.

Publicly Available Information

Not all consumer or customer data is private or sensitive in nature. For example, under the Safeguards Rule[2] the Federal Trade Commission (FTC) defines a customer's information as publicly available if it appears in federal or state government records[3] or in widely distributed media.[4] Examples of such media include information from a telephone directory, newspaper, or website that is available on an unrestricted basis.[5]

---

[1] The Role of Technology in Mortgage Lending (fdic.gov)
[2] eCFR :: 16 CFR Part 314 -- Standards for Safeguarding Customer Information
[3] 16 CFR 314.2(o)(1)(i)
[4] 16 CFR 314.2(o)(1)(ii)
[5] 16 CFR 314.2(o)(3)(ii)

You can also claim a reasonable basis to believe that information is publicly available if it is the type that would be typically available to the public.[6] For example, a reasonable basis can exist to believe that mortgage information is publicly available if you determine that the information is of the kind included in the public record where the mortgage is recorded.[7]

Lastly, if the information is within the customer's power to direct not be disclosed to the public and the customer has not done so, such as having a publicly listed telephone number instead of electing to make it private, that can be considered publicly available information.[8]

You have no legal obligation to safeguard publicly available information from disclosure.

Nonpublic Personal Information

Nonpublic personal information (NPI) includes personally identifiable information (PII).[9] It also includes lists, descriptions, and other groupings of consumers that comes from using PII that is not publicly available,[10] but does not include such lists, descriptions, and other groupings if they are derived from non-publicly available PII.[11] PII is information that permits directly or indirectly inferring the identity of an individual. It includes information that is linked to or can be linked to that person.[12]

NPI also includes lists, descriptions, and other customer groupings that you might assemble by using PII that is not publicly available.[13]

PII includes:

- information that a consumer provides on an application for a financial product or service[14]
- information about a consumer that comes from any transaction with the consumer that involved a financial product or service[15]
- information about a consumer obtained in connection with providing a financial product or service.[16] This can include information about loans,[17] account balances or payment information,[18] information that a person is or has been a customer[19] or suggests the same,[20] information obtained from consumer reports,[21] and information gained from tracking the customer with Internet "cookies."[22]

---

[6] 16 CFR 314.2(o)(2)(i)
[7] 16 CFR 314.2(o)(3)(iii)(A)
[8] 16 CFR 314.2(o)(2)(ii)
[9] 16 CFR 314.2(l)(1)(i)
[10] 16 CFR 314.2(l)(3)(i)
[11] 16 CFR 314.2(l)(2)(ii)
[12] What is Personally Identifiable Information? | Homeland Security (dhs.gov)
[13] 16 CFR 314.2(l)(3)(ii)
[14] 16 CFR 314.2(n)(1)(i)
[15] 16 CFR 314.2(n)(1)(ii)
[16] 16 CFR 314.2(n)(1)(iii)
[17] 16 CFR 314.2(n)(2)(i)(A)
[18] 16 CFR 314.2(n)(2)(i)(B)
[19] 16 CFR 314.2(n)(2)(i)(C)
[20] 16 CFR 314.2(n)(2)(i)(D)
[21] 16 CFR 314.2(n)(2)(i)(G)
[22] 16 CFR 314.2(n)(2)(i)(F)

Some specific examples of PII include:[23]

- names
- addresses
- Social Security numbers
- driver license numbers
- passport numbers
- alien registration numbers
- income
- account numbers
- payment histories
- loan or account balances
- biometric data
- criminal histories
- medical records
- financial records

Under federal law, financial institutions – including mortgage lenders[24] – owe certain duties to their customers about the NPI of those customers in its possession. These duties include giving a privacy notice to anyone with whom you have established a customer relationship.

Consumers Versus Customers

It is important to distinguish between consumers and customers. This is because your obligations to protect their data are different in some ways.

Consumers

A consumer is an individual, not a legal entity like a company, who obtains a financial product or service primarily for personal, family, or household purposes.[25] An individual who applies for a loan like a home mortgage can be a consumer even if the loan is not approved.[26]

Customers

A customer is a consumer with whom you have established a continuing relationship.[27] Customers include those who have obtained loans, [28] including mortgage loans.[29] They also include individuals who enter into an agreement or understanding with you under which you arrange or broker a home mortgage loan for the consumer.[30]

Who is a customer does not depend on the frequency of that person's interactions with the lender or the duration of their relationship. For example, no matter how many times a person uses an ATM at a bank where that individual does not have an account, no customer relationship exists.[31] A former customer is also a consumer.[32]

For mortgage brokers and loan originators, who is a customer and who is a consumer can also depend on who owns the mortgage loan and who services it. This distinction can become important if a

---

[23] How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act | Federal Trade Commission (ftc.gov)
[24] 16 CFR 314.1(b)
[25] 16 CFR 314.2(b)(1)
[26] 16 CFR 314.2(b)(2)(ii)
[27] 16 CFR 314.2(e)(1)
[28] 16 CFR 314.2(e)(2)(i)(B)
[29] How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act | Federal Trade Commission (ftc.gov)
[30] 16 CFR 314.2(e)(2)(i)(E)
[31] How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act | Federal Trade Commission (ftc.gov)
[32] Id.

mortgage loan originator sells the mortgage loan: the continuing customer relationship with the customer is the servicing relationship. For example, if a mortgage loan originator sells the loan and does not retain servicing rights to it, the new servicing company will have the customer relationship with the mortgage holder and the loan originator would have a consumer relationship.[33]

The Current Information Security Threat Environment

Information security requires attention to multiple areas of possible vulnerability. Threats to customer data and to your organization can come from different sources, have different motivations, and involve different means. They can come from hackers on the other side of the planet, or from inside one of your branch offices. They can be planned, automated attacks on your computer systems, or take the form of a link in an otherwise innocent-looking email or text message to an employee. They can be intentional, or careless. They can be clumsy and easy to spot, or so sophisticated that you may not know for weeks or even months that they happened; according to an annual study in 2022 it takes an average of 277 days to discover and contain a data breach, with 212 days being the average detection time.[34]

Unauthorized Disclosures of Customer Information

A person's right to personal privacy includes a reasonable expectation of privacy in that individual's personal data. This privacy expectation includes the assumption that those who have custody of personal data will safeguard it from unauthorized access or from misuse by those who have access. As we will see, the federal government and many state governments require financial institutions, including mortgage loan originators, to protect the personal data of their customers and employees.

The first step toward reducing the risk of having a data breach happen to you is to understand the nature of the threats you face. These you can break down into two categories: potential threat actors inside and outside your company, and the main avenues to gain unauthorized data access: stolen credentials, vulnerability exploits, and botnets.[35]

Sources of Information Security Threats

People are the main source of security incidents and data breaches. In 2022 four of every five data breaches involved a human element.[36] The twin wellsprings of most unauthorized access to sensitive customer data are human error and human avariciousness. People inside your company and people on the outside are both capable of failing to safeguard customer data or improperly accessing it.

Insider Threats

In the financial and insurance industries organizational insiders were involved in about one-quarter of data breaches in 2022.[37] Although disgruntled workers or others holding a grudge are involved in about one percent of these breaches,[38] mistakes and lax security policies are the most common way that people inside a mortgage company compromise customer data. Mistakes are responsible for about 15

---

[33] 16 CFR 314.2(e)(2)(ii)(B)
[34] IBM Security, Cost of a Data Breach Report 2022 at p. 14
[35] 2022 Data Breach Investigations Report | Verizon
[36] 2022 Data Breach Investigations Report | Verizon
[37] 2022 Data Breach Investigations Report | Verizon
[38] 2022 Data Breach Investigations Report | Verizon

percent of data breaches.[39] Errors can include mis-delivery of information to unauthorized recipients, misconfiguring data storage systems, and accidental publishing of customer data.[40]

The most common expression of lax data protection is poor password security: In 2018, for example, about 80 percent of hacking-related data breaches took advantage of stolen or weak passwords. About 70 percent of employees at all businesses admit to re-using passwords at work even though 90 percent also recognize that doing so is poor security practice.[41]

Another common way that employees can put their own companies at risk is through casual information sharing practices with mortgage applicants. Mortgage lenders are not alone in experiencing the tug-of-war between ensuring maximum data security and trying to make the customer's experience as easy and fast as possible. Instructing customers on how to send documents through more secure portals can be time-consuming, and some customers may resist using them in favor of the unencrypted platforms they are comfortable with. Efforts to please customers by cutting corners with their data privacy come at an increasing risk today. Still, according to a 2014 survey of mortgage lenders, 70 percent of lenders small and large were allowing mortgage applicants to send personal and financial information to the company through unencrypted email.[42]

Outsider Threats

Seven of 10 times someone attempts to gain unauthorized access to your customer data, that person will be someone outside of your company.[43] Of these outsiders, 95 percent have financial motivations, and four percent are trying to spy on your company.[44] It is possible for outsiders to work with current or former employees of your company to gain access, such as by obtaining passwords from them.[45]

Security Events, Incidents, and Data Breaches

Information security professionals rate the severity of attacks on networks and data loss on three levels:[46]

- Events: An event describes most any activity on a network, including sending emails or web page access requests. An unsuccessful attempt to guess a password or a phishing scam email that goes directly to spam without being read are events, as are legitimate uses of the network. The FTC defines a "security event" as an event that results in unauthorized access to, disruption of or misuse of an information system, information stored on it, or customer information the company holds in physical form.[47]

---

[39] 2022 Data Breach Investigations Report | Verizon
[40] 81% Of Company Data Breaches Due to Poor Passwords - Bank of North Dakota (nd.gov)
[41] Id.
[42] https://www.halock.com/halock-investigation-finds-70-mortgage-lenders-putting-sensitive-financial-data-risk-application-processes/
[43] 2022 Data Breach Investigations Report | Verizon
[44] Id.
[45] Consumers' data leaked by ex-mortgage workers – Baltimore Sun
[46] 2022 Data Breach Investigations Report | Verizon
[47] 16 CFR 314.2(p)

- Incidents: An incident is an event that compromises the integrity, availability, or confidentiality of a network or its components.[48] A security incident puts any kind of data at risk of disclosure. A privacy incident is a security incident that has the potential to disclose NPI.[49]
- Breaches: A data breach is a security incident that results in data disclosure.[50]

How Data Breaches Happen

Attempts to penetrate your customer data safeguards can be random but are often sophisticated and involve three basic steps: reconnaissance, initial compromise, and exploitation.

- Reconnaissance: Outside threat actors will often seek to identify people in your organization to target, using publicly available information. Social media platforms are one such information source that hackers frequent. The purpose of the reconnaissance is to identify individuals and their roles in the company so that the outsider threat can use that information to craft an initial compromise strategy.
- Initial compromise: The outsider's initial approach to the company will frequently involve tactics collectively known as "social engineering." Social engineering takes what the outsider learned from reconnaissance to approach a targeted individual while masquerading as a trusted source. This can be an email from someone the victim wrongly believes is a coworker, supervisor, or other partner in business. The email can include a fake invoice for payment or request the victim to take some other action by clicking on a link. The link serves to introduce malware into the company's computer network, which in turn can compromise additional network user credentials and bypass internal security measures to access customer NPI.
- Exploitation: Given the average delay time between the initial compromise and when it is detected, an outsider with unauthorized access to the company's network and its customer data can have weeks or even months to operate undetected. During this interval, the outsider will seek to expand the initial compromise into other parts of the company network and may install ransomware to lock out employees from customer data by encrypting it. Malicious outsiders will sometimes attempt to extort a victim company repeatedly. For example, the first demand may be for money to decrypt ransomware installed on the network. A follow-up extortion attempt can be to demand more payment to return stolen data coupled with a threat to disclose it.

Stolen Credentials

Stolen or compromised user credentials are the most common source of data breaches. In 2021 and 2022 stolen or compromised credentials were used in one of every five data breaches.[51] A troubling aspect of credentials-based breaches is that they take the longest of any kind of data breach to detect and correct – more than 320 days on average, including more than 240 days to identify them.[52] This gives the hacker more time to exploit after the initial compromise.

Phishing

Successful attacks on computer networks often are the result of hackers who use tactics proven over the years to work. These include "phishing scams" or attacks which try to persuade the recipient of a

---

[48] 2020 DBIR Cheat Sheet | Verizon Enterprise Solutions
[49] Is It an Incident or a Breach? Defining the Difference (integrity360.com)
[50] Id.
[51] IBM Security, Cost of a Data Breach Report 2022 at p. 6
[52] Id.

communication to give away customer NPI or to obtain network user identity and login information. After stolen and compromised credentials, phishing is the second most prevalent source of data breaches at about 15 percent.[53] It is also the costliest on average, at almost $5 million per breach incident.[54]

A commonly used phishing scam is an email claiming that the user's account password must be reset or claiming that the user's account has a problem and providing a link to supposedly fix it. Some bolder phishing attempts include one or more phone calls to the intended victim to increase the perceived legitimacy of the request.

Phishing attacks can target large numbers of people, but hackers can apply them selectively. A "spear phishing" attack is one that targets a specific individual. "Whaling" is a term that describes a hacker's approach that targets an executive-level person in the company.[55]

Another kind of credentials-based attack targets the home buyer instead of the mortgage lender. Real estate fraud, also known as mortgage fraud, can occur when an outsider does reconnaissance on the buyer and the lender as they negotiate the loan. Near closing the outside party pretending to be a broker, real estate agent, mortgage representative or attorney involved in the transaction will send a communication to the home buyer that mimics a legitimate communication, such as changed money wire transfer request that routes funds to an account controlled by the cybercriminal.[56]

Vulnerability Exploits

In a computer network a vulnerability is a weakness in the system that a cybercriminal can compromise to attack the network. This can be outdated software because the company has not kept up with incremental upgrades or patch fixes, or account access policies that are too permissive. Vulnerabilities include misconfigurations, unsecured application programming interfaces, and software "zero day" flaws known to threat actors but not to the company. Vulnerability exploits rank third after credentials and phishing as the source of data breaches, comprising about 13 percent annually.[57]

Botnets

A botnet is created when malicious software, like a computer virus, takes control over a network of devices. Online hackers often use botnets to attack other networks in support of ransomware attacks, stealing or destroying data, or to damage the victim by degrading its competitive advantage or harming its reputation.[58] Botnets are a problem for older networks that use password-based access portals. They are quickly becoming a significant issue for mortgage companies. In 2021 malicious botnet attacks were 25 percent of reported transactions by U.S. mortgage lenders.[59] This is up from two percent in 2019.[60]

---

[53] Id.
[54] Id
[55] What Is Social Engineering in Cyber Security? - Cisco
[56] How to Avoid Mortgage Wire Fraud - Experian
[57] IBM Security, Cost of a Data Breach Report 2022 at p. 17
[58] What Is a DDoS Attack? Distributed Denial of Service - Cisco
[59] The True cost of Fraud™ Study | LexisNexis Risk Solutions p.17
[60] Id.

Mortgage Cybercrimes as White-Collar Crimes

Cybercrimes involving mortgages are a form of white-collar crime. They are not violent crimes but target the victim financially.[61] The federal government agencies that combat white-collar crime in mortgage lending can vary depending on the nature of the criminal activity.

For example, the Federal Bureau of Investigation (FBI) considers two kinds of mortgage fraud to be white-collar crimes: fraud for profit, in which people involved in the home purchase steal cash and equity from lenders and homeowners, and fraud for housing, which involves deceptive buyers who attempt to mislead lenders about their means or to manipulate property values.[62]

The FBI coordinates with other government agencies to investigate mortgage fraud. It also plays a leading role in investigating another crime that is often connected with fraudulent mortgage activities: money laundering.[63] When the FBI considers it appropriate it will coordinate with other agencies to de-conflict cases.[64] What this means is that the FBI can agree to let other agencies take the lead in investigating and prosecuting mortgage-related cybercrimes outside of mortgage fraud. This is where other federal agencies, including the Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB), can play prominent roles.

White collar crimes are sometimes referred to as victimless crimes, but that is not true. Although the theft and misuse of consumer and customer data may not involve violence against its victims or society, it still causes financial, reputational, and emotional harm that can resonate beyond the simple hacking of an account.

The Unlawful Uses of Compromised Data

The value to cybercriminals of stolen customer or consumer NPI lies in how they can monetize it. Someone who hacks into your network and steals the NPI of your customers may have little or no interest in manipulating their victims' accounts with you. Instead, the data thief can use the data to for unjust enrichment or to conceal their own identities behind someone else's.

Unjust enrichment motivations include applying for loans or credit cards, making fraudulent purchases, filing fraudulent tax returns, fraudulently claiming government benefits, medical prescription fraud, accessing bank accounts, and even extortion in the form of ransomware attacks.[65] Identity theft using stolen customer data can be used to confuse law enforcement when a criminal is arrested and uses a fake ID with the victim's PII, or applies for housing or employment in the victim's name.[66] Finally, stolen information can be sold to others so they, too, can take advantage of it.[67]

The Harm Data Breaches Cause in Mortgage Lending

It is hard to understate the gravity of the threats that financial institutions face from breaches of customer data security. Some recent statistics provide an understanding of how pernicious and costly it is to mortgage companies and their customers:

---

[61] White-Collar Crime — FBI
[62] Id.
[63] Id.
[64] Id.
[65] What Do Hackers Do with Stolen Information? - Experian
[66] Id.
[67] Id.

- Online fraud attempts are pervasive. Every month mid-to-large size mortgage lenders experience about 1,500 cyber-attacks.[68] The financial and insurance sector reported more than 2,500 cyber incidents in 2021, with almost 700 confirmed data breaches. Of these, one-quarter of the threat actors were internal to their organizations.[69]
- Fraud occurs in all parts of the mortgage customer journey. The three areas where fraud losses occur are in new account creation, account login, and funds distribution.[70] Distribution of funds is the area most susceptible to fraud, but unauthorized account logins account for most fraud-related losses.[71]
- People are the biggest source of data breaches. It is tempting to think of information security as being about software and hardware and information technology, but four of every five data breaches involve a human element.[72]
- The cost of fraud is significantly more than the value of a fraudulent transaction. Fraud costs include those connected with its aftermath, including investigatory costs, legal fees, recovery expenses, and more. According to one study, with every dollar of a transactional mortgage lending fraud loss comes more than three dollars in additional costs.[73]
- Cybersecurity-related losses cost mortgage lenders billions of dollars annually. The cost to the mortgage banking industry from cybersecurity-related losses in 2021 was almost $7 billion, with a cost per stolen record of about $175.[74] Mortgage lending fraud costs increased by more than 20 percent from 2020 to 2022.[75]

The need for vigilance among mortgage lending professionals against unauthorized disclosure of customer data through data breaches remains evergreen.

The Information Security Statutory and Regulatory Framework

The federal government and many state governments have recognized the privacy risks posed to consumers by the proliferation of electronic NPI data, much of it being stored on the "cloud" – internet servers that can be accessed from anywhere through gateway devices and applications. This awareness of the problem has translated into laws and regulations that put requirements on companies that gather and store consumer and customer information to safeguard the privacy of that data and to keep customers and consumers informed of their data privacy rights.

---

[68] The True cost of Fraud™ Study | LexisNexis Risk Solutions
[69] 2022 Data Breach Investigations Report | Verizon
[70] The True cost of Fraud™ Study | LexisNexis Risk Solutions
[71] Id.
[72] 2022 Data Breach Investigations Report | Verizon
[73] Id.
[74] Webinar Materials: Mortgage Cybersecurity Update (richeymay.com)
[75] The True cost of Fraud™ Study | LexisNexis Risk Solutions

The Gramm-Leach-Bliley Act

In 1999 the federal government passed the Gramm-Leach-Bliley Act (the GLB Act).[76] The GLB Act limits how a financial institution can disclose consumer NPI to third parties.[77] A mortgage broker or mortgage lender is a financial institution under the GLB Act.[78]

The FTC and the CFPB both have authority under the GLB Act to make and enforce regulations that affect how financial institutions protect consumer and customer privacy:

- The FTC privacy regulations are known as the "Financial Privacy Rule."[79]
- The CFPB privacy regulations are referred to as "Regulation P."[80]
- The FTC regulations requiring information security programs are known as the "Safeguarding Rule."[81]

The Financial Privacy Rule

Although it used to be broader in application, today the Financial Privacy Rule applies mainly to automobile dealerships. The Financial Privacy Rule retains references to mortgage brokers,[82] but the policy of the FTC appears to be to defer to the CFPB and to Regulation P to enforce privacy protection requirements on mortgage companies. [83]

Regulation P

The CFPB administers consumer and customer privacy disclosures through Regulation P. Title X of the Dodd-Frank Act gives rulemaking authority under the GLB Act to the CFPB for financial institutions that are subject to CFPB jurisdiction.[84] Regulation P applies to mortgage loan originators, lenders, and servicers[85] [86] to whom consumers provide NPI to in attempting to qualify for a loan.[87]

Specifically, Regulation P sets the rules that govern a financial institution's responsibility to provide notices to consumers and customers and to limit disclosure of NPI.[88]

---

[76] https://www.govinfo.gov/content/pkg/PLAW-106publ102/html/PLAW-106publ102.htm
[77] How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act | Federal Trade Commission (ftc.gov)
[78] 16 CFR 314.1(b)
[79] eCFR :: 16 CFR Part 313 -- Privacy of Consumer Financial Information
[80] 12 CFR Part 1016 - Privacy of Consumer Financial Information (Regulation P) | Consumer Financial Protection Bureau (consumerfinance.gov)
[81] Document (ftc.gov)
[82] See 16 CFR 313.3(i)(2)(i)(D) and 16 CFR 315.5(b)(2)(ii)
[83] 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."*
[84] 102016_cfpb_GLBAExamManualUpdate.pdf (consumerfinance.gov)
[85] 12 CFR 1016.1(b)(1)
[86] 12 CFR 1016.3(l)(3)(ii)(K)
[87] 12 CFR 1016.3(e)(2)(ii)
[88] Id.

Regulation P applies to mortgage brokers and mortgage lenders in their capacities as financial institutions that are significantly engaged in financial activities.[89] A mortgage broker that formally engages with consumers and customers, and which is regularly engaged in lending or brokering activities, qualifies as a financial institution.[90]

Initial privacy notices to non-customer consumers

- If you do not disclose consumer NPI to any non-affiliated third party and you do not have a customer relationship with the consumer, then you do not have to provide an initial privacy notice.[91]
- If you intend to disclose consumer NPI to a non-affiliated third party, then outside of a few exceptions you must provide the consumer with an initial privacy notice before making any disclosure.[92] Generally speaking, a nonaffiliated third party is anyone who is not an affiliate or employee of yours.[93]
- The exceptions referred to above include information sharing required to process or administer a consumer-requested transaction.[94] Disclosures required for fraud-prevention purposes,[95] or to comply with federal or state laws[96] also do not require a consumer privacy notice.
- It is permissible to give non-customer consumers a "short form" notice that explains that the full privacy notice is available on request, describes a reasonable way for a consumer to get the full privacy notice, and includes an opt-out notice.[97]

Initial privacy notices to customers; revised notices

- You must provide a required initial notice to a customer when you enter a customer relationship[98] or within a reasonable time after the customer relationship begins if the creation of the customer relationship happens without the election of the customer[99] or if waiting to provide the notice would substantially delay the customer transaction and the customer agrees to receive the initial notice later.[100]
- For financial institutions, the customer relationship begins when the loan originates or when an institution purchases the servicing rights to the loan.[101]

---

[89] 12 CFR 1016.3(l)(3)(i)
[90] 12 CFR 1016.3(l)(3)(ii)(K)
[91] 12 CFR 1016.4(b)(1)
[92] 12 CFR 1016.4(a)(2)
[93] 12 CFR 1016.3(o)(1)
[94]12 CFR 1016.14(a)
[95] 12 CFR 1016.15(a)(2)(ii)
[96] 12 CFR 1016.15(a)(7)(i)
[97] 12 CFR 1016.6(d)
[98] 12 CFR 1016.4(c)(1)
[99] 12 CFR 1016.4(e)(2)(i)
[100] 12 CFR 1016.4(e)(2)(ii)
[101] 12 CFR 1016.4(e)(2)(i)(A)

- For an existing customer who obtains a new financial product or service, you can provide a revised privacy notice.[102] [103] 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.[104]

Annual 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.[105]
- 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,[106] or if you have not changed your privacy policies and procedures since the most recent privacy notice given to the customer.[107] 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[108] 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.[109]

Content of notices

If you must provide an initial, annual, or revised privacy notice to a consumer or customer, then you must provide it in clear and conspicuous form.[110] The notice must include at a minimum the following elements of information:

- The kinds of NPI you collect[111] and the kinds of NPI you disclose.[112] This includes NPI obtained from a consumer reporting agency or disclosure of information like names, addresses, phone numbers, and account balances.
- 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.[113] This information can include financial services providers, insurance companies, mortgage brokers, nonprofit organizations, and direct marketers. 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.[114]

---

[102] 12 CFR 1016.4(d)(1)
[103] eCFR :: 12 CFR 1016.8 -- Revised privacy notices
[104] 12 CFR 1016.4(d)(2)
[105] 12 CFR 1016.5(a)(1)
[106] 12 CFR 1016.5(e)(1)(i)
[107] 12 CFR 1016.5(e)(1)(ii)
[108] 12 CFR 1016.5(e)(2)(ii)
[109] 12 CFR 1016.5(e)(2)(ii)
[110] 12 CFR 1016.6(a)
[111] 12 CFR 1016.6(a)(1)
[112] 12 CFR 1016.6(a)(2)
[113] 12 CFR 1016.6(a)(3)
[114] 12 CFR 1016.6(a)(5)

- An explanation of 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.[115] Partial opt-outs, in which the consumer or customer can select which nonaffiliated third parties may receive NPI, are acceptable.[116] A reasonable means to opt out can include a toll-free telephone number,[117] or a detachable form with a check-off box and mailing information.[118] A procedure that requires a customer or consumer to write a letter to opt out, without any other option, is not a reasonable means.[119] Customers and consumers can exercise their opt-out rights at any time.[120] It is your responsibility to comply with an opt-out request as soon as you reasonably can.[121] An opt-out request is effective until the customer or consumer cancels it in writing, or electronically if the customer agrees to that means.[122] If a former customer enters into a new transaction with you, then you must provide the customer with a new opt-out notice that applies only to the new transaction.[123]
- Your policies and practices to protect the confidentiality and security of NPI.[124] These must include a general description of who is authorized to access NPI[125] and state whether you have security practices and procedures in place to ensure confidentiality of information in accordance with your policy.[126] Although it is not necessary to describe your policies and practices in technical detail,[127] 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.[128] [129]
- Disclosures you make to nonaffiliated third parties who are subject to exceptions.[130] If you disclose NPI under an exception to the notice requirements, although you are not required to identify the parties you can state that you make disclosures to other nonaffiliated companies for everyday business purposes, such as to process transactions, maintain accounts, respond to court orders or legal investigations, or to report to credit bureaus.[131]

---

[115] 12 CFR 1016.6(a)(6)
[116] 12 CFR 1016.10(c)
[117] 12 CFR 1016.7(a)(2)(ii)(D)
[118] 12 CFR 1016.10(a)(3)(i)
[119] 12 CFR 1016.7(a)(2)(iii)(A)
[120] 12 CFR 1016.7(h)
[121] 12 CFR 1016.7(g)
[122] 12 CFR 1016.7(a)(2)(ii)(C)
[123] 12 CFR 1016.7(i)(2)
[124] 12 CFR 1016.6(a)(8)
[125] 12 CFR 1016.6(c)(6)(i)
[126] 12 CFR 1016.6(c)(6)(ii)
[127] Id.
[128] Mortgage Company Settles Data Security Charges | Federal Trade Commission (ftc.gov)
[129] Complaint (ftc.gov)
[130] 12 CFR 1016.6(a)(9)
[131] 12 CFR 1016.6(c)(2)(ii)

Regulation P includes a Model Privacy Form.[132] 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.[133]

To sum up Regulation P, you may not yourself nor through any affiliate disclose consumer or customer NPI to a nonaffiliated third party unless:[134]

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

The FTC Safeguarding Rule

Ensuring that consumers and customers are aware of their NPI privacy rights and have the right to opt out of disclosures of NPI to unaffiliated third parties is half of the responsibility that financial institutions have to their customers. The other half is to take active measures to safeguard consumer and customer information in their custody. This is the province of the FTC Safeguarding Rule.

All financial institutions subject to the GLB Act are also subject to the Safeguarding Rule, including mortgage brokers and lenders.[135] The Safeguarding Rule identifies consumers, customers, publicly available information, PII and NPI in the same way this module does in its *"What is Customer Data?"* section; the regulatory references in that section are to Safeguarding Rule provisions.

The most significant aspect of the Safeguarding Rule is its requirement for financial institutions to develop, implement, and maintain a comprehensive information security program (ISP).[136] The purposes of an ISP are to ensure the security and confidentiality of customer information, to protect it against threats to its security or integrity, and to defend against unauthorized access to information that could lead to substantial harm or inconvenience to a customer.[137]

In December of 2021, the FTC issued a final rule that amended the Safeguarding Rule, including changes to ISP requirements. Some of these changes will take effect on December 9, 2022.[138] Where applicable we identify these changes below. Also, some of the ISP requirements do not apply to financial institutions that maintain consumer information for fewer than 5,000 customers. We identify those as well.[139]

An ISP must include all the following elements:

- A designated qualified individual. The qualified individual oversees, implements, and enforces the ISP. A qualified individual can be an employee, an affiliate employee, or a third-party service provider.[140] If you use an affiliate employee or service provider, then you must designate a

[132] Appendix to Part 1016 - Model Privacy Form | Consumer Financial Protection Bureau (consumerfinance.gov)
[133] 12 CFR Appendix to Part 1016 B.1.(b)
[134] 12 CFR 1016.8(a)
[135] 16 CFR 314.1(b)
[136] 16 CFR 314.3(a)
[137] 16 CFR 314.3(b)
[138] 16 CRF 314.5
[139] 16 CFR 314.6
[140] 16 CFR 314.4(a)

senior person in your company to provide direction and oversight of the qualified individual and require the qualified individual's organization to have its own ISP that conforms to the Safeguards Rule.[141] [*Effective December 9, 2022*]

- A written risk assessment. The risk assessment must identify reasonably foreseeable internal and external threats to the security, confidentiality, and integrity of customer information that could lead to its unauthorized disclosure, misuse, alteration, destruction, or other compromise.[142] The assessment must also assess the adequacy of existing safeguards against such unauthorized activity. The assessment must include the criteria by which you identify threats, state how you determine your information system confidentiality and integrity considering those threats and describe how you will mitigate or accept risks based on the assessment and show how your ISP will address those risks.[143] [*The requirement for risk assessments to be in writing begins on December 9, 2022. It also does not apply to companies with fewer than 5,000 customers in their information systems.*]
- Risk assessment-based safeguards [*Effective December 9, 2022*]. These include:
    - periodic reviews of access controls, limiting system access to authorized users and further limiting authorized user access to information they need to do their job duties; also limiting customer system access to their own data.[144]
    - identifying and managing data, people, devices, and systems that your organization must rely on to do business and tailoring the ISP to them.[145]
    - when possible encrypting customer information during transmittal and while in storage or if that is not possible securing it by an effective alternative that the ISP qualified individual reviews and approves.[146]
    - if you use your own applications to store, access, or transmit customer information, implementing secure practices to develop, test, and evaluate the security of those applications.[147]
    - using multi-factor authentication for people who access the company's information system, unless the ISP qualified individual approves in writing access controls that are reasonably equivalent to or better.[148]
    - a data retention policy for securely disposing of customer information no later than two years after the information is last used in connection with the financial product or service unless a lawful business or legally required exception applies; and a procedure to periodically review the data retention policy.[149]
- Regular system monitoring and testing. This includes system controls and procedures to detect unauthorized attempts attack the system or intrude into it.[150] Monitoring and testing must be done continuously or, if continuous monitoring is not possible, on a periodic basis [*Effective*

[141] Id.
[142] 16 CFR 314.4(b)
[143] Id.
[144] 16 CFR 314.4(c)(1)
[145] 16 CFR 314.4(c)(2)
[146] 16 CFR 314.4(c)(3)
[147] 16 CFR 314.4(c)(4)
[148] 16 CFR 314.4(c)(5)
[149] 16 CFR 314.4(c)(6)
[150] 16 CFR 314.4(d)(1)

December 9, 2022; the continuous monitoring requirement also does not apply to companies with fewer than 5,000 customers in their information systems].[151] Periodic testing must include annual system penetration testing and vulnerability assessments every six months, and must also be done when the information system is materially changed or when you believe the information system may have been affected by a material impact, such as an attempted attack.[152]

- Knowledge and training policies and procedures [*Effective December 9, 2022*]. The ISP must provide for personnel security awareness training, updated as necessary to adapt to threats found in risk assessments. Those personnel responsible for managing the company's information systems must be qualified to do so, and the ISP must provide for their qualifications and current and ongoing training.[153]
- Overseeing service providers. The ISP must provide for reasonable steps to select and train service providers to maintain system safeguards and to periodically assess those providers, not only to assess how well they are safeguarding the information systems but also to assess the risks they may pose to the company.[154] [*Requirement to periodically assess service providers becomes effective December 9, 2022*]
- Ongoing evaluations. The ISP must evaluate and adapt to risks and threats that system monitoring and testing and risk assessments reveal. It must also adapt to changes in the way you do business or to any other circumstances that you know or have reason to know will affect your ISP.[155]
- A written incident response plan [*Effective December 9, 2022; also, does not apply to companies with fewer than 5,000 customers in their information systems*]. The purpose of the incident response plan is to help you to respond to and recover from a security event that materially affects the confidentiality, integrity, or availability of customer information in your system.[156] The incident response plan must address the following specifics:
    - The plan goals.[157]
    - Internal processes to respond to a security event.[158]
    - Clearly defined roles, responsibilities, and levels of decision-making authority.[159]
    - Internal and external communications and information sharing.[160]
    - Requirements to remediate identified weaknesses in information systems and controls.[161]
    - Procedures to document and report security events and related response activities.[162]

---

[151] 16 CFR 314.4(d)(2)
[152] 16 CFR 314.4(d)(2)(ii)
[153] 16 CFR 314.4(e)
[154] 16 CFR 314.4(f)
[155] 16 CFR 314.4(g)
[156] 16 CFR 314.4(h)
[157] 16 CFR 314.4(h)(1)
[158] 16 CFR 314.4(h)(2)
[159] 16 CFR 314.4(h)(3)
[160] 16 CFR 314.4(h)(4)
[161] 16 CFR 314.4(h)(5)
[162] 16 CFR 314.4(h)(6)

    - Procedures to evaluate security event responses and revise the incident response plan accordingly.[163]
- Regular internal reporting [*Effective December 9, 2022; also, does not apply to companies with fewer than 5,000 customers in their information systems*]. The qualified individual must report at least annually to your board of directors or equivalent organizational governing body, or to a senior officer responsible for the ISP if no governing body exists.[164] The report must detail the overall status of the ISP, the company's compliance with the Safeguarding Rule, risk assessments, risk management and control decisions, arrangements with service providers, system testing results, security events and how management responded to them, and recommended changes to the ISP.[165]

Remedies and Penalties for GLB Act Violations

The FTC[166] and the CFPB[167] 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.[168] 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.[169]

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.[170] A state law that provides more consumer and customer protections than the GLB act is consistent with the GLB Act.[171]

FTC and GLB Red Flag ID Theft Detection Plans

In addition to Regulation P and the Safeguarding Rule, financial institutions including mortgage lenders[172] must comply with identity theft protections that are known as the "Red Flag Rule."[173] The Red lag Rule requires financial institutions to implement a written Identity Theft Prevention Program, appropriate to the size and complexity of the company,[174] to spot the early warning signs of identity theft. An Identity Theft Prevention Program includes the following elements:

---

[163] 16 CFR 314.4(h)(7)
[164] 16 CFR 314.4(i)
[165] Id.
[166] How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act | Federal Trade Commission (ftc.gov)
[167] 12 USC Sections 5481(12)(J), 5514(b)-(c), and 5515(b)-(c)
[168] https://www.govinfo.gov/content/pkg/BILLS-107s450is/html/BILLS-107s450is.htm
[169] 18 U.S. Code § 3551 - Authorized sentences | U.S. Code | US Law | LII / Legal Information Institute (cornell.edu)
[170] 15 USC 6807: Relation to State laws (house.gov)
[171] Id.
[172] 16 CFR 681.1(b)(3)(i)
[173] eCFR :: 16 CFR Part 681 -- Identity Theft Rules
[174] 16 CFR 681.1(d)(1)

- The program must have policies and procedures to identify relevant red flags for the financial institution's covered accounts and build those red flags into the program.[175] A covered account includes a mortgage loan.[176]
- The program policies and procedures must detect red flags that have been built into the program.[177]
- The program must respond appropriately to detected red flags to prevent and mitigate identity theft.[178]
- The program must be updated periodically to consider changes to customer risks and to the safety and soundness of the ability of the financial institution to guard against identity theft.[179]

Like the requirements for an Information Security Plan, an Identity Theft Prevention Program requires approval by the board of directors of the financial institution[180] and involve the board or a senior manager in overseeing, developing, and administering the program[181] and in training staff to implement it.[182]

Examples of red flags include:

- Alerts, notifications, or warnings from consumer reporting agencies.[183]
- Suspicious documents. These can include documents with evidence of having been forged or altered, identification photographs that appear inconsistent with the appearance of a loan applicant, or an application that gives the appearance of having been forged or altered.[184]
- Suspicious personal identifying information. This can include addresses that do not match any found in a consumer report, an applicant who has no Social Security number, using a Social Security number belonging to someone else, invalid phone numbers, fictitious addresses, and failing to provide all requested forms of identification.[185]
- Unusual or suspicious use of an account. These kinds of activities can include using an account in a way inconsistent with established patterns of activity, mail sent to the account holder being repeatedly returned an undeliverable, notification of unauthorized charges, material changes in spending patterns, and recent nonpayment of an account with no history of missed or late payments.[186]
- Receiving notices from customers, ID theft victims, law enforcement authorities, or others about possible identity theft connected with covered accounts the financial institution holds.[187]

---

[175] 16 CFR 681.1(d)(2)(i)
[176] Fighting Identity Theft with the Red Flags Rule: A How-To Guide for Business | Federal Trade Commission (ftc.gov)
[177] 16 CFR 681.1(d)(2)(ii)
[178] 16 CFR 681.1(d)(2)(iii)
[179] 16 CFR 681.1(d)(2)(iv)
[180] 16 CFR 681.1(e)(1)
[181] 16 CFR 681.1(e)(2)
[182] 16 CFR 681.1(e)(3)
[183] 16 CFR Appendix A to Part 681 VII.(d)1.
[184] 16 CFR Appendix A to Part 681 VII.(d)5-9.
[185] 16 CFR Appendix A to Part 681 VII.(d)10-18.
[186] 16 CFR Appendix A to Part 681 VII.(d)19-25.
[187] 16 CFR Appendix A to Part 681 VII.(d)26.

The SAFE Act

As we have seen earlier, not all incidents of financial institution customer data breaches come from outside the financial institution. About one-quarter involve one or more people within the institution. Many of these breaches may be accidental or inadvertent, but some are the result of intentional behavior.

The Secure and Fair Enforcement for Mortgage Licensing Act (the SAFE Act), which became law in 2008, helps to promote consumer confidence in the integrity of mortgage lending professionals.[188] It does this by maintaining a registry of mortgage loan originators (MLOs), the Nationwide Mortgage Licensing System (NMLS) and Registry.[189] MLOs who are licensed and registered as a state-licensed MLO and who meet the minimum eligibility threshold of acting as the capacity of an MLO for more than five mortgage loans in a 12-month period must register for and maintain annually a unique identifier in the NMLS.[190]

Financial institutions subject to the SAFE Act must provide information to the NMLS Registry to obtain an NMLS identification number,[191] including the employment status of each of its MLOs.[192] If an MLO ceases to be an employee, the financial institution must notify the NMLS Registry within 30 days of the end of the employment relationship.[193]

Financial institutions subject to the SAFE Act must keep written policies and procedures and conduct annual independent compliance tests to ensure that the policies and procedures comply with the SAFE Act and its implementing regulations.[194] The policies and procedures must:

- Establish a process to identify which employees must be registered with the NMLS Registry
- Require all MLOs to be informed of SAFE Act registration requirements and be instructed on how to comply with them
- Establish procedures to comply with SAFE Act unique identifier requirements
- Establish reasonable procedures to confirm the adequacy and accuracy of MLO registrations
- Provide for appropriate actions if an MLO does not comply with registration requirements, including prohibiting such employees from acting as MLOs and other appropriate disciplinary actions
- Establish a process to review employee criminal history background reports, including actions to take under SAFE Act regulations and other applicable federal laws and to maintain records of reports and actions taken
- Establish procedures to make sure that third parties with which the financial institution has MLO-related ties also have policies and procedures to comply with the SAFE Act and its regulations.

---

[188] 12 U.S.C. 5101
[189] Getting Started: MLO (nationwidelicensingsystem.org)
[190] 12 U.S.C. 5103(a)
[191] 12 CFR 1007.103(e)
[192] 12 CFR 1007.104(b)
[193] Id.
[194] 12 CFR 1007.104

The SAFE Act sets forth the minimum requirements for an MLO to be state-licensed. These include completion of at least 20 hours of pre-licensing education,[195] passing a qualified written examination,[196] meeting surety bond requirements, not having had a loan originator license revoked anywhere, not having been convicted or having pled guilty to a felony-level crime, and otherwise demonstrating financial responsibility and fitness of character to warrant community confidence in the MLO's honesty, fairness, and efficiency.[197] The registration process includes a background check.[198]

The CFPB has authority to enforce the SAFE Act, including the summons and examination authority. [199] If the CFPB finds a violation of the SAFE Act has occurred it can issue cease-and-desist orders,[200] hold hearings related to those orders,[201] issue temporary orders, and assess monetary penalties of up to $25,000 violation.[202]

Information Security Best Practices

The central pillars of protecting consumer and customer privacy are understanding the federal and state laws that govern your responsibilities and having policies and procedures in place to safeguard data while complying with statutory and regulatory requirements. In this last section we will cover some best practices to help you to create an effective Information Security Plan for your company.

There are many sources of information you can use to help create a good ISP and to keep up with the latest changes in consumer privacy and cybersecurity laws. The FTC's CyberWise Tips site condenses lessons learned from CFPB Cybersecurity Team experience.[203] The FTC also maintains online guides to help businesses protect customer information,[204] understand how the Safeguarding Rule works,[205] apply the Red Flags Rule,[206] reduce the vulnerability of information systems,[207] and respond to data breaches.[208]

We will use the FTC's top 10 security recommendations here.[209]

1. Make security a factor in your entire business decision-making process. Information security should not be an afterthought in your business day-to-day operations, but an integral part of them. Make conscious and deliberate choices about the kinds of information you collect, who can access it, and how long you keep it.
2. Establish sensible controls over data access. Only those employees with a legitimate business need in your company should have access to customer NPI, and then only on a need-to-know

---

[195] 12 U.S.C. 5104(c)
[196] 12 U.S.C. 5104(d)(2)
[197] 12 U.S.C. 5104(b)
[198] 12 U.S.C. 5104(a)
[199] 12 U.S.C. 5113
[200] 12 U.S.C. 5113(c)(1)
[201] 12 U.S.C. 5113(c)(2)
[202] 12 U.S.C. 5113(d)(2)
[203] Cybersecurity CyberWise Tips | Consumer Financial Protection Bureau (consumerfinance.gov)
[204] https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business
[205] https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know
[206] https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business
[207] https://www.ftc.gov/business-guidance/resources/security-check-reducing-risks-your-computer-systems
[208] https://www.ftc.gov/business-guidance/resources/data-breach-response-guide-business
[209] Start with Security: A Guide for Business | Federal Trade Commission (ftc.gov)

basis. Establishing user accounts to limit access to sensitive information can reduce unauthorized access, as can keeping customer physical records under lock and key.

3. Require secure passwords and authentication. Strong passwords can help to defeat attempts to steal or guess them. Also, make sure that any written records of passwords, if you keep any, are stored securely. Use multi-factor authentication if possible, instead of password-only system access.
4. Store NPI securely and protect it during transmission. Encrypted storage and data transmission are sound practices. It is acceptable to use service-provider experts who have experience with industry-tested and accepted methods of keeping data secure. Also, train your employees to resist the temptation to make convenience-based decisions with customer data, especially in its transmission, such as by using unencrypted email to receive customer NPI.
5. Segment your network and monitor who accesses it. A well-configured information system with multiple computers and devices can segregate parts of the network from other parts through internal firewalls and different levels of user access. This can reduce the risk of unauthorized access to NPI. Also, monitoring network access can identify anyone who may be trying to get to NPI or other data that the person does not have a legitimate need to access so that you can take corrective action.
6. Limit remote access. Many employees work from home or work in the field. You may also have third party service providers who can access your information systems. Restrict the people and the kinds of devices they use that have remote access through account restrictions and restricting network access to specified IP addresses.
7. Make sure your service providers are secure. It does little good to secure your own network if hackers can get at it through a service provider who accesses your information systems without adequately securing its own.
8. Test and verify your compliance. Once you have your security measures in place, make sure that your employees are using them and using them properly. System access monitoring and penetration testing are good tools to spot weaknesses and correct them before a data breach occurs.
9. Keep your software up to date. Threats to your information systems are always changing, and your network and anti-virus software must keep up to match evolving threats. Software that is out of date is more vulnerable to hacking, so having a policy to regularly update and patch your software is a good insurance policy against system intrusions.
10. Dispose of physical medium data securely. Record destruction, physical and electronic, must be done in a way that an opportunistic person in or outside of your company cannot reconstitute it. Burning, shredding, or pulverizing documents and media like hard drives and flash drives are effective ways to prevent inadvertent compromise of data.

Conclusion

The information security and data disclosure threat environment that mortgage lending professionals face today is unparalleled. Not only can a data breach cost your business severely in terms of money, reputational damage and even its survival, but it can also lead to sanctions from the FTC or the CFPB. If you adopt information security and customer NPI data disclosure policies and procedures that comply with the requirements of federal and state requirements, you can reduce the risk of a damaging breach but also avoid penalties that can cost you even more. Staying current with Regulation P, the

Safeguarding Rule, and the SAFE Act are three keys to keeping your information security vulnerabilities and risks to the lowest possible level.

-30-

Quiz

1. Which of the following is not true about the distinction between consumers and customers?
    a. A person can be a consumer or a customer, but not both.
    b. All customers are consumers.
    c. A customer has an ongoing relationship with you.
    d. A former customer can be a consumer.

    Answer: A

2. Which of the following best describes the relationship between non-public personal information and personally identifiable information?
    a. Personally identifiable information is publicly available.
    b. Personally identifiable information is a type of non-public personal information.
    c. You only have a duty to protect personally identifiable information, not non-public personal information.
    d. Personally identifiable information is separate from non-public personal information.

    Answer: B

3. Which of the following is least likely to be considered as personally identifiable information?
    a. A Social Security number
    b. A person's address
    c. A phone number listed in a telephone directory
    d. An individual's address

    Answer: C

4. Which of the following is true about the customer relationship between a mortgage lender and the customer?
    a. The customer relationship stays with the original lender, even if it sells the mortgage.
    b. Who is the customer depends on who owns the loan, regardless of who services it.
    c. The customer relationship follows the servicer of the loan if the loan is sold.
    d. If the original lender sells the mortgage, a customer relationship exists between the customer and both the seller and buyer of the loan.

    Answer: C

5. An outsider who targets one or more individuals in your company to approach with an attempted phishing scam is engaged in what kind of behavior?
    a. Exploitation
    b. Initial compromise
    c. Whaling
    d. Reconnaissance

    Answer: D

6. Which of the following is not an example of a vulnerability exploit?
    a. Outdated software
    b. Malicious software
    c. Misconfigured software
    d. A zero-day software flaw

    Answer: B

7. Which of the following is true about privacy notices to consumers or customers?
    a. If an existing customer buys a new product or service from you, your last notice to the customer will suffice as long as you gave it within the last 12 months.
    b. You must provide annual notices to consumers until you have removed their data from your information system under your record retention and destruction policy.
    c. You must send a revised privacy notice to consumers if your data sharing policy changes within 12 months after your last contact with them.
    d. You only need to send annual notices to current customers.

    Answer: D

8. Which of the following is not considered to be a reasonable way to require a customer to opt out of sharing that person's data with unaffiliated third parties?
    a. A toll-free telephone number to call.
    b. Instructing the customer to write a letter to the company, with no other option.
    c. A detachable form with an opt-out checkbox and instructions on where to mail the form.
    d. An online website where the customer can go to, or instructions on where to write a letter to the company.

    Answer: B

9. Which of the following is one of the purposes of the SAFE Act?
    a. To encourage consumer confidence in the integrity of mortgage lending professionals.
    b. To establish ISP plan requirements for financial institutions.
    c. To protect consumers and customers from unauthorized disclosures of their PII.
    d. To register customers who opt out of having their NPI disclosed.

    Answer: A

10. Which of the following is not part of an information security plan?
    a. Registering all MLO employees with the NMLS Registry.
    b. Regular system monitoring and testing.
    c. Ongoing evaluations.
    d. Designating a qualified individual.

    Answer: A