WORLD LIBRARIES

Volume 25

No. 1

2021 worldlibraries.dom.edu/index.php/worldlib |

Consumer Privacy Practices and Tech in the Title Insurance Industry: A Case Study of First American Title Company

Natasha M. Wojcicki

Dominican University

ABSTRACT

Title companies issue title insurance policies to protect owners and lenders from unknown defects to real property. The title and closing process involves the collection, use, and disclosure of consumer personal information that is managed by technology systems and

web applications. While this helps title companies collaborate with customers, it also makes them targets to cybercriminals. Title companies follow industry best practices to safeguard consumer data. First American Title Company, one of the nation's leading title insurance companies and a leader in e-commerce application systems, was evaluated to better understand the privacy practices of title companies. Unfortunately, First American suffered a data leak that exposed the personal information of millions of consumers. Since there are no federal data privacy laws, First American has relatively gone unscathed by the incident even though it was a known system vulnerability. Therefore, it is recommended that federal privacy laws be implemented, an oversight agency be established for enforcement, and a privacy by design approach should be used by tech companies when developing their systems.

INTRODUCTION

The success or failure of the title insurance industry in the United States is dependent on the real estate market. Typically, title insurance is issued after a real estate purchase or mortgage refinance transaction in the form of an owner's policy and/or lender's policy. Title insurance serves a valuable purpose by insuring the ownership status of real property "against such problems as unknown recorded liens, defects in public records, forgeries, and improperly delivered deeds" (Sirmans & Dumm, 2006, p. 293). Ownership of real property is often one of the largest monetary investments people make in their lives and title insurance helps to protect people's investment from unknown issues that were not discovered during the title review process. For example, someone claiming to be the real owner of a property or a foreclosure of a mortgage that was not found in the public records.

During the title review and closing processes, title companies are often provided with Non-public Personal Information (NPI) of buyers and sellers ("consumers") contained in various forms and applications, such as mortgage loan documents, settlement statements, and financial

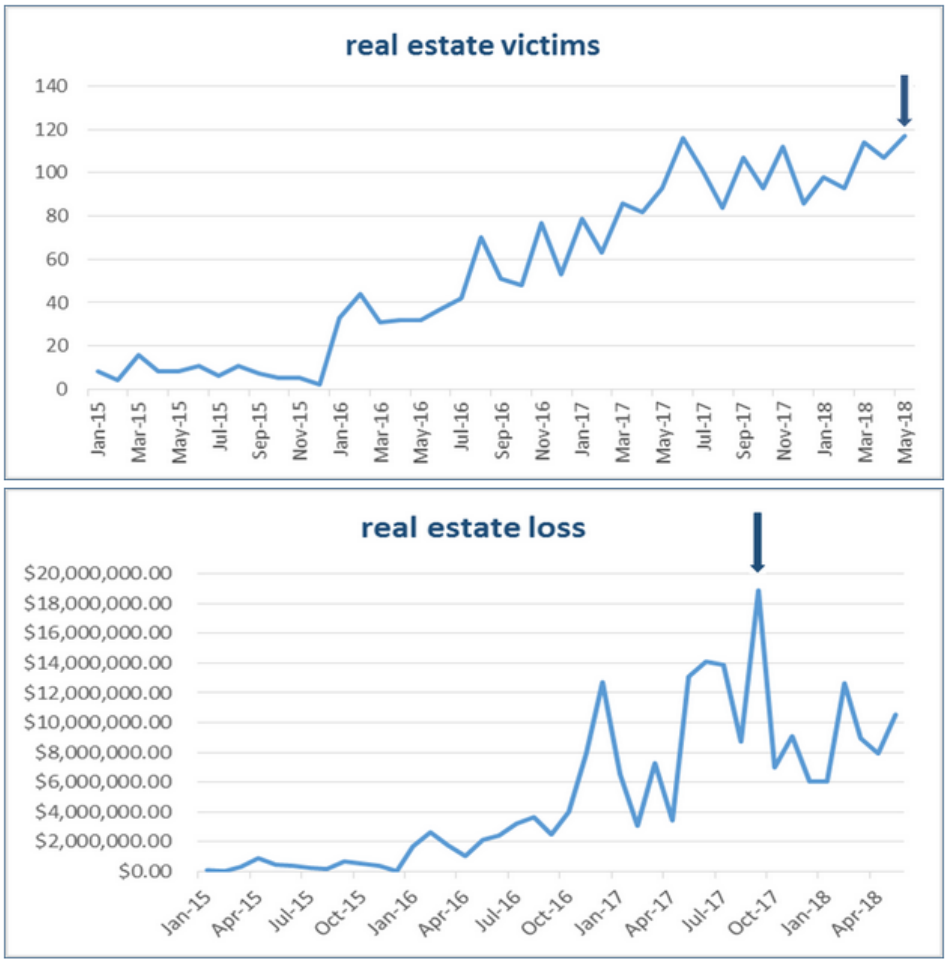
records. According to the best practices framework developed by the American Land Title Association (ALTA), NPI is defined as the "first name or first initial and last name coupled with any of the following: Social Security Number, driver's license number, state-issued ID number, credit card number, debit card number, or other financial account numbers" (ALTA, 2013). As part of the financial services sector, title companies are obligated to follow federal data management legislation and state laws regarding consumer data collection practices, such as the California Consumer Protection Act (CCPA) that became effective on January 1, 2020. One result of legislation has been the creation of privacy policy or notice statements issued to consumers that outlines the collection, use, and distribution of their personal data. Additionally, title companies in many states are obligated to adhere to internet privacy laws that may require businesses to take special measures to secure its information technology infrastructures. This is particularly important in today's digital age where more personal information is going online as part of business operations and processes.

In pursuit to streamline title and closing processes, title companies are investing more in technology solutions for delivering title and closing services through web applications. Title companies understand the increasing demand for electronic communication tools to meet the expectations of a tech-driven culture. This is especially true during the COVID-19 pandemic as title companies are relying more on technology to safely conduct remote closings and online notarizations with customers. Many web applications used by title companies allow certain customers to submit new orders, view and modify file information, access and transmit file documents, search file records, and send electronic messages. Some of the information contained in these web portal systems include NPI, which requires user credentials and strong access controls to be put into place by a title company's technology support team.

As a result of title companies collecting, storing, and distributing NPI, as well as transferring funds from consumers, title companies are a target for cybercriminals. Title companies

reported an increase in email phishing campaigns and business email compromise (BEC) (see Figure 1) by hackers posing as a party on a real estate transaction to obtain personal information to commit fraud. According to the FBI, "wire fraud in real estate is one of the fastest growing cybercrimes in the country. The FBI reportedly received 301,580 complaints in 2017 and losses exceeded $1.4 billion, and in the real estate/rental sector alone, more than 9,600 victims lost over $56 million in the same year" (Neisen, 2018, para. 3). With the high incidence of cyber fraud in the real estate sector, how are title companies protecting the privacy of consumers?

Figure 1. Reported BEC scams reported to the FBI in 2018 (FBI, 2018b).



The aim of this research is to assess the privacy practices of title companies by conducting a case study of First American Title Company. At the end of 2019, First American's revenue was $6.2 billion, making it one of the nation's leading title insurance companies (First American, 2020a). The company is also considered a leader in technology applications with the development of its e-commerce systems for customers (Bell, 2000). Therefore, First American represents the standard by which title companies should follow with respect to consumer privacy best practices.

METHODOLOGY

Case studies are useful to gain insight into a topic using diverse sources, which can lead to more extensive studies in the future. The disadvantages of case studies are that results cannot be generalized to the broader population, may not follow the scientific method, and difficult to draw conclusions of cause and effect. Nevertheless, an exploratory case study of First American Title Company was conducted for this paper to learn more about the title insurance industry and their consumer privacy practices. Information was gathered from journal articles, periodicals, title insurance associations, and title company websites to better understand the topic.

Questions throughout the research process included: What is title insurance? What is the role of title companies like First American? What technology applications do they use and who uses it? What information do they collect, store, and distribute? How do they protect consumer privacy? Who regulates First American and the title insurance industry? What laws and regulations currently exist about consumer privacy that First American must follow? What industry best practice principles or framework guides the business operation and processes of First American?

RESULTS

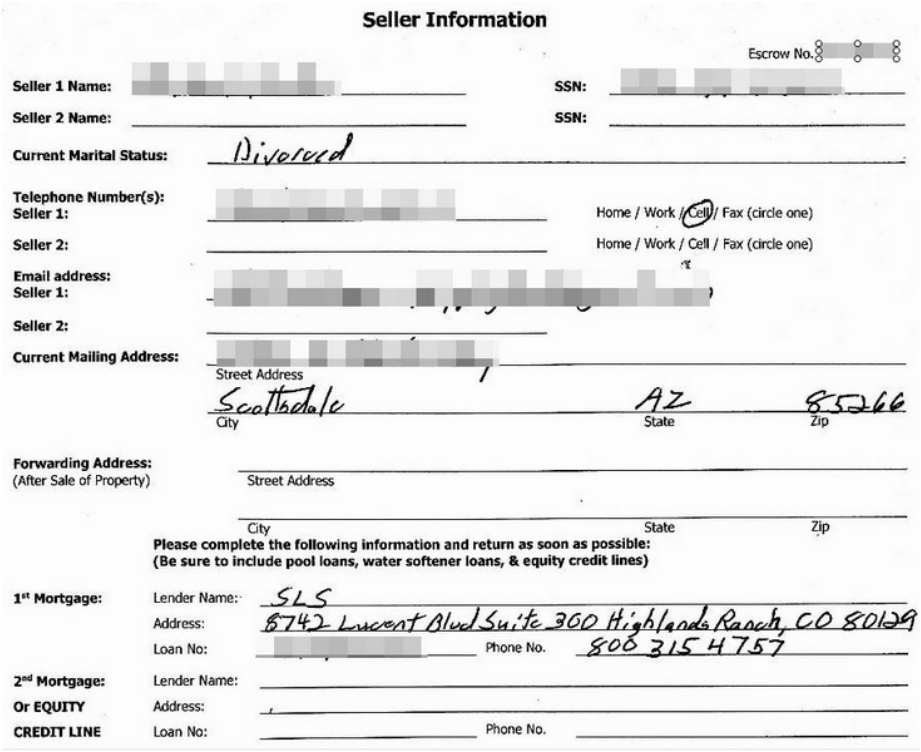
First American has a Privacy Notice posted on their website that acknowledges that the company collects, uses, and shares personal information that is consistent with the company's "Fair Information Values" (First American, 2020b). It applies to information that they receive when individuals use their applications, website, products and/or services, company communications (e.g. phone, email, etc.), and third-party sources. The information collected may contain non-public "personal information" that "can be used to directly or indirectly identify or contact" users (First American, 2020b, para. 13). Some examples listed by First American include names, dates of birth, social security numbers, biometric information, unique online identifiers, ID numbers, financial information, and insurance policy numbers.

The Privacy Notice specifically addresses the company's adherence to the company's Fair Information Values that includes: 1) "fairness" to ensure balance between the benefits that they offer and user privacy; 2) support of an open "public record" because it creates value for society, allows users to have more choices, and creates opportunity; 3) "use" personal information responsibly and adhere to applicable laws like the CCPA; 4) ensures the "accuracy" of the information that the company collects, uses, and shares about users and that they will take reasonable steps to correct inaccurate information; 5) "education" awareness about how employees and the industry should collect, use, and share personal information; and 6) "security" of personal information by using commercially reasonable technical, organizational, and physical protections (First American, 2020b). First American also states that they do not sell the personal information of users to "nonaffiliated" third parties (First American, 2020b, para. 21). However, they do share personal information with subsidiaries, affiliates, and unaffiliated third parties only with the user's consent, in a business transfer like a merger or acquisition, with service providers like credit/debit card companies, subsidiaries and affiliates to ensure consistent operations with applications, website, and products, and for legal purposes and protection (First American, 2020b).

In addition, the Privacy Notice states that they store and protect personal information using commercially reasonable measures. While First American does not specifically state the type of technologies or strategies used to protect personal information, the policy states the they will use their "best efforts to maintain commercially reasonable technical, organizational, and physical safeguards, consistent with applicable law," to protect a user's personal information (First American, 2020, para. 40). Furthermore, the company states that they will store the personal information of users as long as legally necessary and will dispose of it in a secure and proper manner. However, some personal information may be kept indefinitely even after a user's relationship with the company has ended. This not only includes consumers that use First American's title and closing services, but customers like attorneys and lenders who use the company's web application products to access, search, and share documents that may contain NPI.

Despite First American's statements about taking every reasonable step to protect personal information of users, a major data leak was discovered in one of the company's web programs in December of 2018 by a real estate developer named Ben Shoval. When he discovered the system glitch that allowed him to view documents from other files that contained NPI, and without the need for authentication, he contacted First American (Krebs, 2019a). Unfortunately, due to miscommunications that occurred within their technology department, the glitch was not immediately fixed. When Shoval's concerns were not addressed by First American, he contacted cybersecurity journalist, Brian Krebs, who broke the news on his website in May 2019. Krebs (2019b) took the screen shot (Figure 2) of one of the documents he could access to show the seriousness of the situation. The seller's personal information such as name, social security number, phone number, email address, mailing address, and loan number were exposed to unauthorized parties.

Figure 2. Screen shot of a document conatining NPI from Brian Krebs (2019b).



Seller Information

Escrow No. [redacted]

Seller 1 Name: [redacted] **SSN:** [redacted]

Seller 2 Name: _____ **SSN:** _____

Current Marital Status: Divorced

Telephone Number(s):
Seller 1: [redacted] Home / Work / Cell / Fax (circle one)

Seller 2: _____ Home / Work / Cell / Fax (circle one)

Email address:
Seller 1: [redacted]

Seller 2: _____

Current Mailing Address: [redacted]
Street Address
Scottsdale — AZ — 85266
City — State — Zip

Forwarding Address:
(After Sale of Property)
Street Address
City — State — Zip

Please complete the following information and return as soon as possible:
(Be sure to include pool loans, water softener loans, & equity credit lines)

1st Mortgage: Lender Name: SLS
Address: 8742 Lucent Blvd Suite 300 Highlands Ranch, CO 80129
Loan No: [redacted] Phone No. 800 315 4757

2nd Mortgage: Lender Name: _____
Or EQUITY Address: _____
CREDIT LINE Loan No: _____ Phone No. _____

A redacted screenshot of one of many millions of sensitive records exposed by First American's Web site.

After the news went viral, First American disabled the website to stop the data leak of hundreds of millions of records exposing the personal information of consumers. The news of the data leak got the attention of the New York State Department of Financial Services (NYDFS), which investigated and charged First American with violating the State's cybersecurity requirements for financial institutions. An investigation discovered that the glitch occurred due to a system update to the web program in 2014 and that it went undetected until a penetration test in December 2018 (NYDFS, 2020). Consequently, the NPI of consumers was exposed for years until Ben Shoval happened to come across the system vulnerability. The NYDFS and First American are set to meet at a hearing about the charges on October 26, 2020. Thus far, it appears that the NYDFS is the only government entity to charge First American with breaking consumer privacy laws and regulations.

DISCUSSION

The perspective of First American on consumer privacy appears to be one of importance based on statements made in their Privacy Notice. However, the investigation by the NYDFS has shown a major disparity between what First American preaches and what they practice. According to the NYDFS, First American failed to follow its own policies and procedures with respect to protecting consumer data. The company violated not only certain privacy laws and regulations, but the trust of their consumers.

Unfortunately, no federal data privacy laws exist in the United States nor a centralized data protection authority to enforce compliance (Brooks, 2020). The U.S. Federal Trade Commission (FTC) is the only federal agency that has "the power to enforce data protection regulations and protect data privacy" (Brooks, 2020, para. 2). Instead, states have taken on the responsibility of enacting data privacy regulations like the CCPA, New York Consumer Privacy Act, Standards for The Protection of Personal Information of Residents of the Commonwealth of Massachusetts, and the Minnesota Government Data Practices Act (Brooks, 2020). It is the role of state attorneys to enforce compliance. However, it looks like changes are on the horizon with respect to data privacy protection laws since the passing of the EU's General Data Protection Regulation (GDPR) in 2018. The GDPR is arguably the strongest consumer data privacy laws in the world and it has received attention by consumer privacy advocates. It is only a matter of time before the U.S. will have to address data privacy protections, especially as more personal information is being electronically stored.

As a result, the title insurance industry needs to review their industry best practices and enforce the policies to ensure consumer data is protected. The challenges that many title companies face when trying to protect consumer data are technical constraints that involve security and operating requirements, finances to maintain the infrastructure and software

programs, cyber threats, and educating employees about consumer privacy data and the potential threats.

RECOMMENDATIONS

The title insurance industry is doing its best to meet the challenges of balancing technology and protecting consumer data. Many title companies follow industry best practices that were developed by ALTA, but there is no legal requirement that enforces these policies and procedures. It is completely voluntary. While some states have enacted data privacy laws to protect consumers from unauthorized disclosure, it is not enough. First American has relatively gone unscathed by the data leak that exposed millions of consumer records. While the NYDFS has formally charged First American with violating its data privacy laws, the outcome for First American is unknown as this time. So are the potential ramifications to the consumers who had their NPI exposed.

It is recommended that First American and other title companies develop a comprehensive information governance program that addresses information privacy and security. It is important that these policies and procedures are implemented company wide and that employees are trained to properly handle the personal information of consumers. Furthermore, a federal data privacy protection law should be enacted that will ensure consumer privacy from organizations, as well as penalties for violations. The current patchwork of state data privacy laws is ineffective to protect the personal information of consumers.

In addition, systems should be designed with consumer privacy in mind. Privacy is not the priority when tech companies develop their systems because the focus is the user experience and aesthetics. Tech companies need to develop their systems with privacy as an important

element of their design. It should prevent unauthorized disclosure of personal information by default rather than forcing consumers to opt-out of privacy agreements.

LIMITATIONS

A limitation of this case study is that First American was the only title company researched and evaluated to determine the privacy practices of the title insurance industry. Therefore, the findings of the study may not be representative of the industry itself. Additionally, research findings were based on information gathered from the literature and applicable websites, such as First American and title insurance industry associations. The case study should be expanded to include other title companies to ascertain the industry's perspective on information privacy and security, as well as formally assess their privacy practices.

CONCLUSIONS

According to the American Land Title Association (ALTA), the title insurance industry reported a net income of $296.4 million with total assets over $9.7 billion in the first quarter of 2020. This is a 39.3% increase when compared to the first quarter of 2019, which saw a net income of $212.7 million (ALTA, 2020). This is the highest first quarter for the title industry since 2006 (ALTA, 2020). Based on these figures, it is apparent that the title insurance industry is an important institution in the United States. Title companies protect owners and lenders from unknown defects to real property by issuing an owner's policy and/or lender's policy.

To streamline the title and closing processes, title companies have embraced technology solutions to help manage title and closing services through web applications that are accessible to customers. This type of technology is becoming increasingly popular as title companies try

to find remote eClosing solutions during the COVID-19 pandemic. The information collected by title companies often contains the Non-public Personal Information (NPI) of consumers. As a result, cybercriminals target title companies to gain access to this personal information to commit fraud. The title insurance industry has addressed this challenge by implementing best practice standards to protect consumer data from unauthorized disclosure.

First American Title Company was the subject of this case study to determine the privacy practices in the title insurance industry and how they protect the personal information of consumers. First American has taken steps to protect consumer data by developing a Privacy Notice that addresses how they manage consumer data. Unfortunately, a data leak discovered in 2019 from a system vulnerability has called into question the privacy practices of title companies. There are no federal data privacy protection laws. Instead, states have taken on the responsibility of implementing data privacy laws. It is recommended that federal data privacy laws be enacted and enforced to protect the personal information of consumers. Oversight agencies should also be created to enforce these laws and apply penalties for violations. Furthermore, tech companies need to develop systems with privacy as part of the design. Protecting consumer privacy should be a priority and steps should be taken in the U.S. to implement regulations similar to the EU's GDPR.

REFERENCES

ALTA. (2013). *ALTA Best Practices Framework: Title Insurance and Settlement Company Best Practices Version 3.0*. https://www.alta.org/best-practices/

ALTA. (2020, June 23). *First Quarter 2020 Title Insurance Industry Market Share Executive Summary*. https://www.alta.org/news/news.cfm?20200623-First-Quarter-2020-Title-Insurance-Industry-Market-Share-Executive-Summary

Bell, J. (2000, March 1). Technology and the Title Insurance Industry: A New Chapter. *National Real Estate Investor*. https://www.nreionline.com/mag/technology-and-title-insurance-industry-new-chapter.

Brooks, R. (2020, July 3). U.S. Privacy Laws: State-Level Approaches to Privacy Protection. *Netwrix Blog*. https://blog.netwrix.com/2019/08/27/data-privacy-laws-by-state-the-u-s-approach-to-privacy-protection/

FBI. (2018a, July 12). Business E-mail Compromise The 12 Billion Dollar Scam. *FBI*. https://www.ic3.gov/media/2018/180712.aspx

FBI. (2018b, July 12). Figure 1. Reported BEC scams reported to the FBI in 2018. *FBI*. https://www.ic3.gov/media/2018/180712.aspx

First American. (2020a, October 22). 2019 Highlights. *First American*. http://investors.firstam.com/investors/overview/default.aspx

First American. (2020b, January 1). Privacy Notice. *First American*. https://www.firstam.com/privacy-policy/index.html

Krebs, B. (2019a, May 24). First American Financial Corp. Leaked Hundreds of Millions of Title Insurance Records. *Krebs on Security*. https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

Krebs, B. (2019b, May 24). Figure 2. Screen shot of a document conatining NPI from Brian Krebs. *Krebs on Security*. https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/

Niesen, A. (2018, July 11). While Cyber Criminals Continue to Target Real Estate Transactions, Take These Protective Measures. *Forbes*. https://www.forbes.com/sites/forbesrealestatecouncil/2018/07/11/while-cyber-criminals-continue-to-target-real-estate-transactions-take-these-protective-measures/#1b68a65563e1

NYDFS. (2020, July 11). Statement of Charges and Notice Of Hearing Against First American Title Insurance Company. *New York State Department of Financial Services*. https://www.dfs.ny.gov/system/files/documents/2020/07/ea20200721_first_american_notice_charges.pdf

Sirmans, G.S. & Dumm, R.E. (2006). Title Insurance: An Historical Perspective. *Journal of Real Estate Literature, 14(3)*, 293-320.