University of Florida Journal of Law & Public Policy

Volume 28 | Issue 3 Article 5

2017

A Landlord's Obligation to Protect the Saensitive Information of Potential and Current Lessees' From Identity Theft

Danielle Drora Greenstein

NOTES

A LANDLORD'S OBLIGATION TO PROTECT THE SENSITIVE INFORMATION OF POTENTIAL AND CURRENT LESSEES' FROM IDENTITY THEFT

Danielle Drora Greenstein[*]

INTRODUCTION

I. IDENTITY THEFT 520
A. *How Does Identity Theft Occur?* 521
B. *Statistics* 523
C. *How to Protect Against Identity Theft* 524

II. STATUTES 526
A. *Electronic Signature Statutes* 526
B. *Misappropriation of Personal Information* 526
C. *Identity Theft and Renting* 526

III. CORPORATIONS WHO WERE VICTIMS OF BREACHES 527
A. *The Home Depot, Inc.* 528
B. *The Target Incident* 531
C. *Possible Legal Standards for Landlords* 533

IV. STORING AND DISPOSING OF SENSITIVE INFORMATION 534

V. SHOULD LANDLORDS SHOULDER THE RESPONSIBILITY OF SAFEGUARDING A POTENTIAL APPLICANT AND A LESSEE'S PERSONAL INFORMATION? 535
A. *Security Software and Encryption* 536
B. *The Safeguards Rule* 537
C. *Identity Theft Insurance* 538

CONCLUSION 539

---

* Danielle D. Greenstein, Esq., graduated from the University of Florida Levin College of Law in May 2017. She dedicates this Note to her parents: Orly and Zeev Greenstein, and her siblings: Nicole, Adam, and Robin Greenstein; thank you for being my stars—we don't always see each other, but I always know you are there for me. Additionally, a special thank you to Professor Michelle S. Jacobs for her invaluable help and guidance in writing this Note.

INTRODUCTION

Lawyers and relators are suggested additions to a real estate transaction when a person is looking to rent a home. Unfortunately, many people try to circumvent having to hire a lawyer or a relator in an effort to save money. What generally occurs is a transaction solely between an unsophisticated landlord and an unsophisticated lessee. This can have consequences manifesting in the form of, but not limited to, an invalid deed, boundary disputes, or identity theft. A lack of safeguards on behalf of an unsophisticated landlord after acquiring personal information from and about a potential lessee can give a third party the opportunity to hack into the unsophisticated landlord's computer and steal what is referred to as sensitive information, including the potential lessee's personal identification and information.

This Note will explore the issue of whether landlords have a legal obligation to safeguard the sensitive information of lessees or potential lessees. If the personal information of the lessee is accessible by third parties, and is used to harm the lessee, how much liability should be attributed to the landlord who had the sensitive information in his possession?

Part I of this Note examines what identity theft is, how identity theft occurs, and the potential measures an individual may take to safeguard themselves from becoming identity theft victims. Part II gives a quick overview of the relevant electronic signature statute that has made it possible for the process of renting a home to be completed on a digital platform. Part III of this Note examines corporations which were victims of identity theft and the emerging laws from the lawsuits that followed. Part IV addresses the duties and obligations landlords should have to a lessee. Part V is where this Note turns mostly theoretical. Given the information already provided in this Note, Part V analyzes whether a landlord should be responsible for taking certain security measures to safeguard the personal identification and information of a current or potential lessee in the landlord's possession. If a landlord has a duty to safeguard a lessee's personal information, what are the measures a landlord should take to protect him or herself from liability?

I. IDENTITY THEFT

Identity theft should not be confused with identity fraud. Identity theft occurs when a thief acquires enough personal information to be able to impersonate another individual.[1] Personal information is defined as "a

1. *What's the Difference Between Identity Theft and Identity Fraud?*, IDENTITYHAWK, http://www.identityhawk.com/Difference-Between-Identity-Theft-and-Identity-Fraud (last

person's first name or initial and last name in combination with" a person's Social Security number, driver's license number, or credit or debit card numbers "when either the name or the data is unencrypted."[2] When an individual has his information stolen, he becomes a victim of identity theft. Other victims that are affected by identity theft, whether it be directly or indirectly, include financial institutions and organizations that were defrauded from the thief's use of a victim's identity.[3]

Identity fraud occurs when a thief creates personal information and identification to make up a fictitious person.[4] This fictitious person is generally used to take out loans or open up lines of credit for the thief; anything that allows the thief to get their hands on a generous portion of money.[5] When it comes to identity fraud, the financial institution, the organization the breach stemmed from, and the consumers of the organization are the usual victims.[6] A landlord may very well use certain pieces of personal information from different lessees to create a new person altogether, allowing the landlord to go ahead and commit identity fraud. However, this Note focuses on identity theft and how a third party may obtain the personal information of a lessee from the possible negligence of a landlord in possessing and maintaining the lessee's personal information.

A. *How Does Identity Theft Occur?*

An individual's Social Security number (SSN), bank account number(s), credit or debit card number(s) and even driver's license number are only a few examples of what constitutes personally identifying information. A third party (thief) can acquire these different pieces of personally identifying information from an individual and profit at their expense.[7] The thief in possession of an individual's personally identifying information most likely has access to money the victim has put away in bank accounts and has the opportunity to make fraudulent charges or open up new lines of credit in the individual's name.[8] There are several known ways a thief can acquire personal information from an

---

visited Sept. 29, 2016) [hereinafter IDENTITYHAWK].

2. Dana J. Lesemann, *It's Not the Breach, It's the Cover-Up - Using Digital Forensics to Mitigate Losses and Comply with Florida's Data Breach Notification Statute*, 82 FLA. B.J. 21, 21 (Feb. 2008).

3. IDENTITYHAWK, *supra* note 1.

4. *Id.*

5. *Id.*

6. *Id.*

7. *Identity Theft*, U.S. DEP'T OF JUST., https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud (last updated Dec. 2, 2016); *see also* IDENTITYHAWK, *supra* note 1.

8. *Identity Theft*, *supra* note 7.

individual.

Dumpster-diving gives a thief access to any non-shredded document that was thrown away.[9] By finding a pre-approved credit card application in a dumpster, a thief can easily acquire a new credit card in the victim's name.[10] Unless the victim regularly checks his or her credit report, it is unlikely the victim will find out that a credit card has been issued under their name until they apply for a new credit card or a loan. By then it may be too late as the damage will have only just begun.

Identity thieves now have the internet at their disposal. Impersonating another person is facilitated by the use of the internet because the thief does not need to physically be present for a transaction to occur.[11] The thief is also able to forgo the process of forging a signature on a receipt.[12] From the comfort of one's living room, one can purchase items from different stores within minutes.[13] Without the need to go from store to store, committing fraud is only a click away.

Phishing occurs when a person creates an e-mail that is designed to resemble that of a legitimate business, institution, or agency in an attempt to have the recipient of the e-mail disclose their bank account information along with other personal information after being led to a counterfeit website.[14] Phishing e-mails are designed to create the impression that there is an immediate risk to any of the financial accounts owned by the recipient of the corrupt e-mail.[15] A person who responds to a phishing e-mail or clicks on the link provided within a phishing e-mail may be putting more than just their financial information at risk.[16]

Crimeware,[17] otherwise known as a keylogging program, may be implanted into the computer that opened the phishing e-mail. Crimeware is an effort to intercept account usernames and passwords and other sensitive information.[18] There are phishing schemes that use computer viruses or worms to disseminate the corrupted e-mail to other people in the victim's contact list, expanding the reach of potential victims and the damage done.[19]

---

9. Jeff Sovern, *The Jewel of their Souls: Preventing Identity Theft Through Loss Allocation Rules*, 64 U. PITT. L. REV. 343, 355 (2003).

10. *Id.*

11. *Id.* at 357.

12. *Id.*

13. *Id.*

14. *Phishing*, BLACK'S LAW DICTIONARY (10th ed. 2014); Anti-Phishing Working Group (APWG), PHISHING ACTIVITY TRENDS REPORT 2ND QUARTER 2016 1, 2 (2016), http://docs.apwg.org/reports/apwg_trends_report_q2_2016.pdf [hereinafter APWG].

15. *Phishing*, *supra* note 14.

16. *See* APWG, *supra* note 14, at 7.

17. APWG, *supra* note 14, at 2.

18. *Id.*

19. *Id.*

Fifty percent of the malicious programs that have been detected by the company VeriSign have keylogging functionality.[20] These malicious programs are used to intercept information from the victim rather than actually pose a direct threat to the computer itself.[21] Keylogger programs are comprised of two files: (1) dynamic link library (DLL), and (2) executable file (EXE).[22] The DLL is the file that makes the recording of a user's keystrokes possible.[23] The EXE installs the DLL file and triggers the keylogging program to start working.[24] Phishers use keylogging programs to intercept a victim's usernames, passwords, and other sensitive information.[25] These programs record a user's keystrokes and then send the recorded log of keystrokes back to the person who installed the program on the victim's computer.[26]

Unsecured wireless networks are a concern because anyone who has a wireless device and is within a certain range may connect to the internet through the unsecured network.[27] Any illegal download performed over an unsecured wireless network appears as if the owner of the wireless network initiated the illegal download.[28] Computers connected to the unsecured wireless network may also be hacked.[29]

There are a variety of ways a thief can steal a person's identity. It is almost impossible to fully protect oneself from identity theft. However, there are several ways to stop identity theft in its tracks before the problem explodes into one that will take years to remedy.

B. *Statistics*

Every year, the Federal Trade Commission (FTC) receives the largest amount of complaints from consumers regarding the crime of identity theft.[30] From 2006 to 2008 there were 11.7 million people that reported being victimized by identity theft, a total of 5% of Americans from the

---

20. Nikolay Grebennikov, *Keyloggers: How They Work and How to Detect Them (Part 1)*, SECURELIST (Mar. 29, 2007, 1:03 PM), https://securelist.com/analysis/publications/36138/keyloggers-how-they-work-and-how-to-detect-them-part-1/.

21. *Id.*

22. Margaret Rouse, *Keylogger (Keystroke Logger or System Monitor)*, TECHTARGET, http://searchmidmarketsecurity.techtarget.com/definition/keylogger (last visited Nov. 1, 2016).

23. *Id.*

24. *Id.*

25. *Id.*

26. Grebennikov, *supra* note 20.

27. Casey G. Watkins, *Wireless Liability: Liability Concerns for Operators of Unsecured Wireless Networks*, 65 RUTGERS L. REV. 635, 660 (2013).

28. *Id.*

29. *Id.*

30. *Identity Theft and Data Security*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/identity-theft-and-data-security (last visited Oct. 29, 2016).

age of 16 years and older.[31] In 2012 there were 12.6 million Americans that reported being victimized by identity theft and incurred an average loss of $365.00.[32] In 2014, the total amount of combined monetary losses by victims of identity theft was greater than $32 million.[33] The amount of identity theft victims and monetary damages will surely increase if corporations and individuals do not take advantage of the protective software available in an effort to take reasonable steps in safeguarding their computer system(s).

Every month there are 411 to 425 brands that are targeted by phishers.[34] In the second quarter of 2016, there was a 61% increase in the amount of phishing sites that were visited as compared to the previous record of the fourth quarter in 2015.[35] The F.B.I.'s Internet Crime Complaint Center (IC3) gives several suggestions on how to avoid being a victim of phishing scams: do not fill out forms that request personal information through email messages; compare the link received in the email to the link you are directed to; go to the official website of a company in a different tab instead of merely clicking on the link provided in the email; and in what may be the best way to avoid being a victim of a phishing scam, directly contact the business that supposedly sent the link to verify whether or not the email was sent through them and is legitimate.[36]

C. *How to Protect Against Identity Theft*

There is no way to be 100% protected from identity theft; however, there are several steps that can be taken to help lower one's risk of becoming a victim of identity theft. Several of these steps are: do not share identity information when it is unnecessary; be cautious when using your computer; when it is no longer needed, shred any document that contains any identifying information; review financial statements and request copies of credit reports.[37]

What happens when a person shares his or her personal information unnecessarily? Someone who should not get their hands on the personal information, does. There are business entities who request a person's SSN

---

31. *Id.*

32. KRISTIN FINKLEA, CONG. RESEARCH SERV., IDENTITY THEFT: TRENDS AND ISSUES 1 (Jan. 16, 2014), https://www.fas.org/sgp/crs/misc/R40599.pdf.

33. INTERNET CRIME COMPLAINT CTR. (IC3), FED. BUREAU OF INVESTIGATION, 2014 INTERNET CRIME REPORT 47 (2016), https://pdf.ic3.gov/2014_IC3Report.pdf [hereinafter IC3].

34. APWG, *supra* note 14, at 2.

35. *Id.*

36. IC3, *supra* note 33, at 44.

37. Sean B. Hoar, *Identity Theft: The Crime of the New Millennium*, 80 OR. L. REV. 1423, 1438, 1440–42 (2001).

merely for record keeping purposes.[38] There is no reason to give one's SSN to anyone who requests it. It is important to ensure that the entity requesting the SSN needs it for more than record keeping purposes, such as a credit or background check.[39]

Safeguards are not only designed for people; they are designed for computers as well. A firewall is meant to run on an individual computer and is used to configure a server and software to restrict unauthorized access to that computer.[40] Keeping a hacker out of your computer is essential, since nowadays, we do everything on our computers from shopping at an online Target store to taking notes in a classroom. For an avid online shopper, it is convenient to save one's credit card information for a quicker check-out process. It is also possible to send money via PayPal to family and friends or businesses.[41] With so many ways to store a credit card number online, it is a hacker's goldmine to find an unprotected computer.

Many documents containing personally identifying information find their way into the trash. It is not uncommon for a thief to go through a residential dumpster to see if they will get lucky in finding un-shredded documents with such personally identifying information within. All non-essential documents should be shredded prior to being thrown out. A non-essential document should be considered any document that is not required by law or policy to be retained by an individual or business.[42]

Reviewing financial statements for any anomalies helps stop identity theft in its tracks. Merely being aware of when a financial statement is supposed to arrive is a big step in preventing identity theft. If a statement is missing from its billing cycle, there is the possibility that a thief was able to change the billing address in an effort to avoid detection.[43] After noticing the missing financial statement, the quicker a person reports the anomaly to their bank or credit card company the quicker identity theft may be stopped.[44]

Periodically requesting a copy of your credit report is another safety precaution a person may take in the fight against identity theft. Finding an unauthorized account or change made to the account is a big red flag that one's identity may have been stolen or it could just mean that a company accidentally charged the account; however, it is always better

38. *Id.* at 1438.

39. *Id.*

40. Robert Craig Waters, *An Internet Primer for Florida Legal Researchers*, 70 FLA. B.J. 12, 26 (Nov. 1996); *see, e.g.*, Hoar, *supra* note 37, at 1440 n.79.

41. *PayPal User Agreement*, PAYPAL (July 27, 2017) https://www.paypalobjects.com/webstatic/ua/pdf/US/en_US/ua.pdf.

42. Hoar, *supra* note 37, at 1441.

43. *Id.* at 1442.

44. *See id.* at 1443.

to be safe rather than sorry and investigate the unauthorized account or change without any delay.[45]

II. STATUTES

A. *Electronic Signature Statutes*

The first electronic signature act to come into effect was the 1999 Uniform Electronic Transaction Act (UETA).[46] Section 7 of UETA provides that "a record or signature may not be denied legal effect or enforceability solely because it is in electronic form."[47] UETA was the first act which allowed documents to be created by electronic means.[48] Now, e-signatures are enough to satisfy the required signature formality.[49] UETA was a big step in the push for having transactions occur solely online instead of in person and through paper documents. Lessees have the option of signing their rental application and returning it to the landlord online via email.

B. *Misappropriation of Personal Information*

Section 817.5685 makes it "unlawful for a person to intentionally or knowingly possess, without authorization, the personal identification information of another person . . . stored in digital form."[50] Personal identification information takes the form of a SSN, a driver's license number, bank account numbers, and credit and debit card numbers.[51] A person who misappropriates the personal identification information of less than five people has committed a misdemeanor of the first degree.[52]

C. *Identity Theft and Renting*

There are no set regulations for individuals who want to put their home, apartment, or an individual bedroom up for rent. A landlord is

45. *Id.*

46. *Uniform Electronic Transactions Act*, NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS 1 (1999), http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf [hereinafter UETA].

47. UETA, *supra* note 46 at 26.

48. *Id.*

49. Spencer Hale, *Real Property E-conveyances and E-recordings: The Solution or Cause of Mortgage Fraud*, 5 OKLA. J.L. & TECH. 44, at 3–4 (2009), http://www.digitalcommons.law.ou.edu/cgi/viewcontent.cgi?article=1037&context=okjolt.

50. FLA. STAT. § 817.5685(2) (2017).

51. *Id.* § 817.5685(1).

52. *Id.* § 817.5685(3)(a).

concerned with filling up their unused space and getting paid. One of the first things a landlord would ask from a potential lessee is for a completed application form. This application form is used to assess whether or not the applicant will be a safe bet or a risky investment. To determine the kind of risk the applicant is, a landlord will usually perform a credit check.[53] There are companies out there that tailor their services and credit checks specifically to landlords.[54] On the rental application, a potential lessee will generally need to include their name along with other information. For the landlord to be able to perform a credit check, the potential lessee would need to give his or her SSN. The SSN, along with the applicant's name, makes up the foundation of the sensitive personal information that a third party can use to open up new lines of credit or take out loans under the guise of the applicant.

If the rental application is being handed to the landlord as a hardcopy, the applicant would want to stress that once the landlord has no use for it, the landlord should shred the document. Unfortunately, not many people own nor use a shredder. If the landlord was to merely throw out the rental application after performing a credit check, then a thief may happen to come across it while dumpster-diving.

If the applicant is emailing the rental application to the landlord, then it is important for the applicant to ensure the landlord is protecting him or herself with anti-malware programs. A semi-sophisticated hacker would be able to breach the firewalls on an unprotected computer and obtain the rental application with the potential lessee's sensitive information. This would be easier than taking candy from a baby. There is no need to address the consequences an applicant would suffer if a landlord was to fall prey to phishing because hopefully, at this point in time, none of us are clicking any links we receive via email.

III. CORPORATIONS WHO WERE VICTIMS OF BREACHES

There is no shortage of individuals who have reported having their personal information stolen from a hack against a bank, a college, or even a hospital.[55] The Identity Theft Resource Center (ITRC) has been tracking data breaches since 2005.[56] The year 2015 is ranked as the

53. *Rental Laws: 3 Types of Landlord Fraud*, APARTMENT RATINGS (Jan. 16, 2010), http://ohmyapt.apartmentratings.com/rental-laws-3-types-of-landlord-fraud.html.

54. *Credit Check for Landlords*, EXPERIAN, https://connect.experian.com/credit-check/landlords.html (last visited Dec. 13, 2016).

55. Amanda Draper, *Identity Theft: Plugging the Massive Data Leaks with a Stricter Nationwide Breach-Notification Law*, 40 J. MARSHALL L. REV. 681, 686 (2007).

56. *Identity Theft Resource Center Breach Report Hits Near Record High in 2015*, IDENTITY THEFT RESOURCE CTR. (Jan. 25, 2016), http://www.idtheftcenter.org/ITRC-Surveys-Studies/2015databrea ches.html.

second highest year in terms of data breaches, with a total of 781 breaches.[57] Up until 2015, the primary motive for data breaches was financial gain.[58] The year 2015 marked a shift in motive from financial gain to those such as social justice, embarrassing the United States, and compelling certain behavior; however, financial gain is still the primary motive.[59]

The year 2016 has seen several major data breaches. The University of Central Florida (UCF) announced that it was the victim of a hack in February 2016.[60] The data breach at UCF affected about 63,000 current and former students, faculty, and staff whose SSN, first and last names, and student or employee ID numbers were compromised.[61] UCF was not the only school affected this year; both UC Berkeley and Tidewater Community College announced that there was a data breach in their system.[62] UCF recognizes that because personal information was compromised, those affected needed to protect themselves from identity theft. The school offered those that were affected from the breach one year of credit monitoring and identity protection services.[63]

Companies such as LinkedIn and Dropbox have had a data breach from the past come back to haunt them.[64] Both companies downplayed the severity of a breach that occurred in 2012.[65] The past breach was later shown to have affected a larger number of users than was originally thought.[66]

A. *The Home Depot, Inc.*

The Home Depot, Inc., (Home Depot) was the victim of one of the biggest retail hacks in the year 2014.[67] The consumers affected were those who used payment cards in Home Depot's self-checkout terminals.[68]

---

57. *Id.*

58. *Id.*

59. *Id.*

60. Judy Leary, *The Biggest Data Breaches in 2016*, IDENTITYFORCE (Dec. 16, 2016), https://www.identityforce.com/blog/2016-data-breaches.

61. *Id.*

62. *Id.*

63. *UCF Data Breach: 63K Social Security Numbers Compromised*, WESH-TV 1, 2 (Feb. 4, 2016, 4:59 PM), http://www.wesh.com/article/ucf-data-breach-63k-social-security-numbers-compromised/4447239.

64. Leary, *supra* note 60.

65. *Id.*

66. *Id.*

67. *In re* Home Depot, Inc., Customer Data Sec. Breach Litig., No. 1:14MD2583(TWT), 2016 WL 2897520, at *1 (N.D. Ga. May 18, 2016).

68. Jonathan Stempel, *Home Depot Settles Consumer Lawsuit Over Big 2014 Data Breach*, REUTERS (Mar. 8, 2016, 11:33 AM), http://www.reuters.com/article/us-home-depot-breach-settlement-idUSKCN0WA24Z.

Around 56 million Home Depot consumers were harmed when hackers stole their personal and financial information.[69] The stolen consumer information was sold to thieves who ran up a high number of fraudulent transactions on those credit and debit cards.[70]

In the years leading up to the data breach, Home Depot identified the potential repercussions that it would suffer if a data breach would occur.[71] However, Home Depot did nothing to strengthen their data security system to ensure a data breach would be less likely to occur.[72] The information that Home Depot stored in its computer system from consumers who utilized credit and debit cards included the card data, mailing addresses and other personally identifiable information of their customers.[73]

The alleged weaknesses of Home Depot security system included the failure to maintain an adequate firewall, the failure to use coded numbers on its POS terminals, and the failure to update its anti-virus software, among other inadequacies.[74] In the end, hackers were able to breach Home Depot's system due to a firewall flaw.[75] The court determined that due to Home Depot's actions of ignoring any warning signs that a data breach was possible, Home Depot owed an independent duty to its consumers and was able to be sued in tort.[76] The case against Home Depot settled, with the company agreeing to pay at least $19.5 million to the affected consumers.[77]

After all of the data breaches that have occurred and the rise of identity theft since 2015, landlords who store personal information of (potential) lessees should have a duty to ensure that the personal information is safeguarded. The court in the Home Depot case recognized a duty owed to people, which was "not to subject them to an unreasonable risk of harm."[78] There are landlords who are not tech-savvy and do not keep rental applications, most likely containing an applicant's social security number, as well as any background and credit checks that were run, in a secure or encrypted file. By not taking the time to safeguard documents with sensitive information, a landlord may be putting him or herself at risk to be liable to a lessee in tort. Whether or not the lessee can collect on any judgment against the landlord is another question entirely.

As the old adage goes, ignorance of the law is not an excuse.

69. *In re Home Depot, Inc.*, 2016 WL 2897520, at *1.
70. *Id.*
71. *Id.*
72. *Id.*
73. *Id.*
74. *Id.*
75. *Id.*
76. *Id.* at *3.
77. Stempel, *supra* note 68.
78. *In re Home Depot, Inc.*, 2016 WL 2897520, at *3.

Landlords should not be able to claim they were unaware of their duty to not subject their lessees to an unreasonable risk of harm after receiving the application containing the lessee's personal information. Leaving documents with the lessee's personal information in unsecured locations on a computer, or not shredding those documents before throwing them away, increases the likelihood that a lessee's identity may be stolen.

Landlords are in the best position to ensure that the documents in their possession are protected and hard to reach if their computer is hacked. If landlords would be able to escape this duty, as the court in the Home Depot case pointed out, those that are affected by the landlord's negligence would have no substantive remedy available if their identity was stolen and credit card debt and loans were racked up in their name.[79]

The financial institutions affected by the Home Depot security breach were allowed to plead money and interest damages after having to reimburse Home Depot customers for fraudulent charges.[80] Since Home Depot had several opportunities to update its security system and failed to do so, financial institutions were left to bear the grunt of Home Depot's inadequacies. The knowledge of the poor security system in use and Home Depot's failure to heed warnings of possible security breaches created the duty Home Depot owed to the financial institutions.[81] Home Depot serves hundreds, if not thousands, of customers per day. A landlord who rents out property may be dealing with only a handful of lessees. The repercussions of a security breach a landlord experiences if his or her computer is hacked will not reach the same level of damages as a security breach that occurs within a big corporation, such as Home Depot. The landlord is only putting a handful of lessees at risk of having their identity stolen and credit cards and loans taken out in their name. Thus, financial institutions should be able to bear the grunt of reimbursing lessees for any money that was taken out of their account through fraudulent charges through the negligence of landlords. But should financial institutions be responsible for cleaning up after a landlord who was negligent or even reckless in maintaining a lessee's personal information without any reasonable safeguards?

Whether landlords should owe such a duty to financial institutions is most likely a question of fact. Unlike Home Depot, which has a team of employees at its disposal to identify potential threats to its systems, landlords are left to rely on their own technological knowledge. There is no one to put the landlord on notice of the potential for a hack to his or her computer, except for the landlord him or herself. The financial institution that issues the credit card or loan to the identity thief will

79. *Id.* at *4.

80. Melissa J. Sachs, *Financial Institution's Suit Over Home Depot's Data Breach Stands*, 2016 WL 2993627 (N.D. Ga. May 25, 2016).

81. *See id.*

largely be held responsible for the fraudulent transactions. It should come as no surprise that the financial institution would want to shift the burden of repaying the victim of identity theft to the corporation or person who had the means to prevent such theft in the first place.

As the financial institutions in the Home Depot case alleged, there would have been no fraudulent charges for the financial institutions to reimburse, had it not been for Home Depot's failure to adequately secure their computer system.[82] In line with this argument, if a landlord secured the documents containing a lessee's personal information in an encrypted file or took other safety precautions, the financial institution(s) that issued a new credit card or loan to an identity thief under the lessee's name would not have had to pay for the fraudulent charges accrued. The major difference between what happened to consumers at Home Depot and what may happen to a lessee that comes across a negligent landlord is that Home Depot has the deep pockets to cover the losses financial institutions suffer from due to identity theft.

B. *The Target Incident*

Adding to the list of companies that have experienced a data breach is Target. The financial and personal information of 110 million Target customers was stolen.[83] For the hackers that obtained the Target shoppers' information from Target's Point-of-Sale (POS) system, it was a walk in the park. The hackers used an inexpensive variant of a software available on Cybercrime forums to gain access to Target's POS system.[84] Over the course of several weeks these hackers victimized hundreds of Target customers by entering Target's POS system and collecting information ranging from encrypted pin numbers, names, and e-mail addresses.[85] The information collected allowed the hackers, or those that bought the information from the hackers, to use the victims' personal and financial information for fraudulent activity.[86]

The unfortunate fact that Target did not have a secure POS system meant that a customer who once shopped at Target using a credit or debit card was at risk of having their financial and personal information stolen. Some of the customers whose information was possibly stolen had not shopped at Target for over a year.[87] A class action lawsuit was filed

82. *Id.*

83. *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1157 (D. Minn. 2014).

84. Paula Rosenblum, *The Target Data Breach is Becoming a Nightmare*, FORBES (Jan. 17, 2014, 2:22 PM), https://www.forbes.com/sites/paularosenblum/2014/01/17/the-target-data-breach-is-becoming-a-nightmare/#41ddf0c11a35.

85. *Id.*

86. *See In re Target Corp.*, 66 F. Supp. 3d at 1154.

87. Rosenblum, *supra* note 84.

against Target. One of the groups who filed the lawsuit was composed of Target customers.[88] The group of customers alleged unauthorized charges, loss of access to bank accounts, late fees, card replacement fees, and credit monitoring costs.[89] Customers were not the only group affected. The second group that brought a case against Target was composed of financial institutions that were financially impacted due to the Target breach.[90]

Target had a duty to timely disclose to its customers that there was a security breach in which the customers' personal information was compromised.[91] The duty to disclose was created because Target was aware it held sensitive customer information that was compromised. Target's security systems where the sensitive data was stored were inadequately safeguarded, which gave reason for Target to believe that the sensitive information was in fact taken by a third party.[92] The duty to timely disclose is established in section 501.171 of the Florida Statutes.[93] The duty applies to a business entity that collects personally identifiable information from a consumer and keeps it in electronic format.[94] The disclosure of the occurrence of a security breach is required within thirty (30) days of a breach or from the time there was reason to believe a breach had occurred, unless there is no reasonable risk of harm to the owner.[95] Section 501.171 applies to covered entities, which include corporations (such as Home Depot and Target) that maintain, store, or use personal information.[96] The statute does not establish a private cause of action.[97]

Section 501.171 does not cover individual landlords.[98] The argument can be made that because landlords use and may store personal information in electronic format, they should be held liable to a certain extent if the personal information of another that is in their possession was unable to be kept confidential. Landlords should have a duty to disclose to their lessees that their personal information may have been (if there is reasonable belief) or has been stolen. The information in a rental application contains personal information that a landlord should know is considered sensitive information. If the landlord does not encrypt the file in which the application and background or credit checks are kept in, then

88. *In re Target Corp.*, 66 F. Supp. 3d at 1154.
89. *Id.* at 1158.
90. *Id.*
91. *Id.* at 1163.
92. *Id.*
93. FLA. STAT. § 501.171(3)(a) (2017).
94. Personal Data Notification and Protection Act of 2015, H.R. 1704, 114th Cong. § 101(b)(1), 101(c)(2)(A) (2015).
95. § 501.171(4)(a); H.R. 1704 §§ 101(b)(1), 101(c)(2).
96. § 501.171(2).
97. *Id.*
98. *See id.*

the system the sensitive information is maintained in will most likely be considered inadequate by courts. Unfortunately, landlords who fall victim to a hack will most likely be concerned with mitigating their own damages and forget about any duty they may owe to a lessee.

C. *Possible Legal Standards for Landlords*

The cases pertaining to data security breaches within large corporations have ended with settlements. Thus, there is no clear cut legal standard that has arisen to guide other corporations or persons in how to protect the personal identification and financial information of others that is in their possession. However, there has been a pattern of conduct that courts tend to look for in determining liability.

In the Home Depot, Inc., Consumer Data Security Breach Litigation, the state of Alaska rejected an argument to dismiss a claim based on the FTC not explicitly including the maintenance of inadequate security measures as an unfair act.[99] The reasoning behind this is that the FTC's list of unfair practices is not exhaustive but merely illustrative of what an unfair act looks like.[100] Having security measures in place to match the volume of information being maintained and the level of importance being attributed to the information is something courts give great weight to.

Security breaches in corporations affect the financial institutions that the consumer's credit card is linked to. Generally, the financial institution is liable to refund a consumer for fraudulent charges made on his or her credit cards.[101] However, depending on when the consumer reports that his or her credit card information has been stolen may subject the consumer to be liable for a certain amount of the loss.[102] A consumer is not liable for any fraudulent charges if only the credit card number is stolen and not the physical credit card itself.[103] In the Home Depot security breach, the hackers obtained the credit card numbers of consumers.[104] Because the consumers are not liable for the fraudulent

---

99. *In re* Home Depot, Inc., Customer Data Sec. Breach Litig., No. 1:14MD2583(TWT), 2016 WL 2897520, at *5 (N.D. Ga. May 18, 2016).

100. *Id.*

101. FED. TRADE COMM'N, LOST OR STOLEN CREDIT, ATM, AND DEBIT CARDS 2–3 (Aug. 2012), https://www.consumer.ftc.gov/articles/0213-lost-or-stolen-credit-atm-and-debit-cards [hereinafter FTC, LOST OR STOLEN]; *see also* Lindsay Konsko, *Who Pays When Merchants are Victims of Credit Card Fraud?*, NERDWALLET (June 3, 2014), https://www.nerdwallet.com/blog/credit-cards/merchants-victims-credit-card-fraud/.

102. FTC, LOST OR STOLEN, *supra* note 101.

103. *Id.*

104. Paula Rosenblum, *The Target Data Breach Is Becoming a Nightmare*, FORBES (January 17, 2014), https://www.forbes.com/sites/paularosenblum/2014/01/17/the-target-data-breach-is-becoming-a-nightmare/#30dbdf0d1a35.

charges, and the thieves will not pay the financial institutions, the financial institutions must look towards the corporation that was the victim of the hack if they would like to see any of their money returned.[105] This is exactly what happened in the Home Depot case.[106] Similar to corporations who only maintain information about a consumer, a landlord usually never sees the lessee's credit card but only maintains personal information pertaining to that lessee. Financial institutions effected by a landlord's negligence should have some recourse to go after the landlord depending on whether the landlord in good faith tried to safeguard the information he or she had at hand from the lessee.

When a corporation has a large enough security breach that they need to notify over 1,000 persons at a particular time, the corporation is also obligated to notify consumer reporting agencies of the breach.[107] Many landlords do not have over 1,000 lessees at a single time and thus have no real obligation to report the identity theft of their lessee to consumer reporting agencies. By creating an obligation for landlords to report the occurrence of identity theft to consumer reporting agencies, landlords would hopefully take better care in safeguarding the personal information of others due to the added obligation creating another avenue for them to be held liable in the loss of a lessee's personal information.

IV. STORING AND DISPOSING OF SENSITIVE INFORMATION

A landlord has the right to obtain a lessee's SSN to perform credit and background checks in determining whether or not the lessee is a liability.[108] After the credit check is performed, the landlord is in possession of even more sensitive information pertaining to the lessee. Credit and background checks are considered to be consumer reports. Consumer reports are "information obtained from a consumer reporting company that is used—or expected to be used—in establishing a consumer's eligibility for credit, employment, or insurance, among other purposes."[109] The Fair and Accurate Credit Transactions Act of 2003 was passed to combat identity theft through the means individuals use to store

105. *See* Konsko, *supra* note 101.

106. *In re* Home Depot, Inc., Customer Data Sec. Breach Litig., No. 1:14MD2583(TWT), 2016 WL 2897520, at *2 (N.D. Ga. May 18, 2016).

107. MINTZ ET AL., STATE DATA SECURITY BREACH NOTIFICATION LAWS (Sept. 1, 2017), https://www.mintz.com/newsletter/...DataBreachLaws.../state_data_breach_matrix.pdf.

108. *Rental Laws: 3 Types of Landlord Fraud*, APARTMENTRATINGS (Jan. 16, 2010), http://ohmyapt.apartmentratings.com/rental-laws-3-types-of-landlord-fraud.html.

109. FED. TRADE COMM'N, DISPOSING OF CONSUMER REPORT INFORMATION? RULE TELLS HOW (June 2005), https://www.ftc.gov/tips-advice/business-center/guidance/disposing-consumer-report-information-rule-tells-how [hereinafter FTC DISPOSING].

and dispose of a person's consumer report(s).[110] There are several things a landlord should take into consideration when storing and disposing of another person's sensitive information.

After obtaining a credit check, the landlord may want to hold onto the information. How to store such sensitive information is a big consideration. Landlords should store the documents in a secure location with access to only those people that need to know about the information.[111] There is no reason a landlord should share such information with a friend or even a family member.

An individual that uses a consumer report is subject to the Disposal Rule.[112] Landlords should have a method of disposal once the information they received from a credit or background check is not useful to them anymore. The FTC's Disposal Rule outlines several ways a landlord can dispose of a lessee's sensitive information.[113] If a landlord keeps paper files then burning, pulverizing, or shredding papers would be a reasonable way to destroy the documents containing the sensitive information.[114] When documents with sensitive information are kept electronically and are no longer needed, a landlord should destroy or erase the electronic files so that the information cannot be reconstructed.[115] There are programs available to completely wipe certain data from a computer file.[116]

There are consequences for the landlord that knew about the Disposal Rule yet did not take measures to comply with it.[117] A landlord may be obligated to pay a portion of the lessee's unauthorized charges or damages per violation ranging from $100 to $1,000, attorney's fees, and possibly punitive damages.[118] These damages only apply to the landlord that willfully turned his or her back on the safeguards required by the Disposal Rule.[119] What is missing are the repercussions to a landlord who negligently or recklessly handled personal information that caused damage to a lessee.

V. SHOULD LANDLORDS SHOULDER THE RESPONSIBILITY OF

110. Janet Portman, *Handling Tenant Credit Reports: The "Disposal Rule,"* NOLO, http://www.nolo.com/legal-encyclopedia/legal-requirements-handling-tenant-credit-reports-the-disposal-rule.html, (last visited Dec. 10, 2016).

111. *Id.*

112. FTC DISPOSING, *supra* note 109.

113. *Id.*

114. *Id.*; *see also* Portman, *supra* note 110.

115. Portman, *supra* note 110.

116. *Id.*

117. *Id.*

118. *Id.*

119. *Id.*

SAFEGUARDING A POTENTIAL APPLICANT AND A LESSEE'S PERSONAL INFORMATION?

In the Home Depot and Target security breach cases, consumers had their credit card numbers stolen and the thieves racked up fraudulent charges on those credit cards consumers already had out.[120] In a rental application or background or credit check, there is enough information present for a thief to open a new credit card under a lessee's name. This is different from the Home Depot and Target cases because a lessee is not having their credit card number stolen and used elsewhere; there is an entirely new credit card being opened under the lessee's name. The financial institutions affected in the Target security breach case went after Target to reimburse them for their losses.[121]

If a landlord did not take the proper precautions to safeguard the documents containing an applicant or lessee's personal information, then the financial institutions from which the thief applied for new credit cards or took out loans may look to the landlord for indemnification. A landlord does not have the same deep pockets as a multi-million-dollar corporation has. The financial institutions may never recover their judgment against the landlord and will still have to bear the grunt of the financial damage due to the landlord's negligence. If the landlord can prove that he or she took reasonable precautions to guard against a hack, then the landlord should be free from liability.[122] However, if it can be shown that a reasonable person would not have safeguarded the personal information of another in a similar means to that of the landlord, the landlord should be held liable to some extent similar to that of the liability attributed to a landlord in the Disposal Rule.

Having standards to safeguard the documents landlords maintain containing the sensitive information of others would help to decrease the amount of identity theft that occurs. The following are a few suggestions for every landlord who maintains such documents.

A. *Security Software and Encryption*

Having security software installed on a laptop is a great start to fending off third party hackers, especially if the security software updates automatically.[123] If it was up to the landlord to remember when the last

120. *In re* Target Corp. Customer Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1159 (D. Minn. 2014); *see also In re* Home Depot, Inc., Customer Data Sec. Breach Litig., No. 1:14MD2583(TWT), 2016 WL 2897520, at *1 (N.D. Ga. May 18, 2016).

121. Konsko, *supra* note 101.

122. Portman, *supra* note 110.

123. FED. TRADE COMM'N, COMPUTER SECURITY, (June 2017), https://www.consumer.ftc.gov/articles/0009-computer-security.

time he or she updated the security software on his or her laptop, then there would be a lot of confused faces in the crowd. Having security software that updates automatically is beneficial because hackers continue to find new ways to circumvent the present protections on a computer.[124]

Landlords can make sure to educate an applicant in only sending the rental application through an encrypted e-mail or rental website. To ensure that the e-mail or website is encrypted a user should look at the URL bar. If the web address starts off with "https," then the site is encrypted and most likely safe for use in sending personal information.[125] Although one must keep in mind that there is still the possibility that a keylogging program is installed on a computer capable of copying each stroke of the keyboard a user inputs. It is possible to encrypt one's email messages as well.[126] Unfortunately, encrypted email is not foolproof and most people find it difficult to use.[127]

B. *The Safeguards Rule*

Retailers such as Target and Home Depot store their consumer data within their POS systems. Corporations are not held responsible to the same extent as financial institutions are in putting in place safety precautions to avoid becoming a victim of a security breach that harms the consumer.[128] Under the Safeguards Rule, which was issued by the Gramm-Leach-Bliley Act (GLBA),[129] a financial institution is required to have safeguards in place to keep the personal identification and financial information of their customers secure.[130] The purpose of the Safeguards Rule is to "protect the security, confidentiality, and integrity of customer information."[131] The rule lays out the recommended compliance measurements an institution should take to safeguard consumers' personal information.[132]

---

124. *Id.*

125. *Id.*

126. *See* Chris Hoffman, *Why No One Uses Encrypted Email Messages*, HOW-TO GEEK (Apr. 30, 2014), http://www.howtogeek.com/187961/why-no-one-uses-encrypted-email-messages./.

127. *Id.*

128. B. Dan Berger, *Congress Must Make Retailers Responsible for Data Breaches*, AM. BANKER (Jan. 15, 2014, 12:00 PM), http://www.americanbanker.com/opinionbankthink/congress-must-make-retailers-responsible-fo r-data-breaches-1064921-1.html.

129. Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–09 (2012).

130. FED. TRADE COMM'N, FINANCIAL INSTITUTIONS AND CUSTOMER INFORMATION: COMPLYING WITH THE SAFEGUARDS RULE, (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying.

131. FTC Safeguards Rule, 16 C.F.R. § 314.1(a) (2016).

132. Nick J. Vizy, *Safeguards Rule Under the Gramm-Leach-Bliley Act*, 95 RECORDS RETENTION REPORT ARTICLE I (Nov. 2005).

Since the Target breach occurred, many have wondered whether or not Target could have prevented the breach from occurring.[133] Trustmark National Bank and Green Bank NA, both of which filed suit against Target, alleged that Target not only knew about the vulnerabilities in their system that led to the breach, but failed to take any action in updating their system in an effort to save costs.[134] Had the Safeguards Rule applied to corporations such as Target, the security breach that affected so many of Target's customers may not have occurred.

There is no reason why the Safeguards Rule should only apply to financial institutions. The objectives of the Safeguards Rule in obtaining and maintaining security and confidentiality as well as the protection against threats or unauthorized access are in line with protecting the public from harm.[135] Such objectives should be extended to apply to any entity or individual that obtains and maintains another's personal information for business purposes. The Safeguards Rule does not have to apply equally to individuals and corporations as it does to financial institutions, since financial institutions conduct business in large part only after acquiring their customer's personal information.

C. Identity Theft Insurance

Landlords should try to take all reasonable steps necessary to prevent a third party from acquiring any personally identifying information they have on a lessee by using encrypted files and other security measures. If a third party is able to get past any security measure a landlord has in place, the landlord can further protect him or herself from damages by requiring the lessee to have identity theft insurance at the start of the rental period. Identity theft insurance may come in the form of a standalone policy or as part of a package deal to a homeowner's or lessee's insurance policy.[136]

State Farm offers identity theft insurance to lessees which covers the lessee, the lessee's spouse and relatives, and anyone under the age of 21, so long as they live in the lessee's household.[137] There are two types of identity theft insurance: (1) identity restoration case management and (2)

---

133. Emily Coyle, *Target and Security Firm Face Another Security Breach Lawsuit*, THE CHEAT SHEET (Mar. 28, 2014), http://www.cheatsheet.com/business/target-and-security-firm-face-another-security-breach-lawsuit.html/?a=viewall.

134. *Id.*

135. *See* FTC Standards for Safeguarding Customer Information, 16 C.F.R. § 314.3(b) (2017).

136. *Identity Theft Insurance: Tips for Protecting Your Identity*, INS. INFO. INST., http://www.iii.org/article/identity-theft-insurance, (last visited Dec. 11, 2016).

137. *Protect Yourself from the Cost of Identity Restoration*, STATE FARM MUTUAL AUTOMOBILE INS., https://www.statefarm.com/insurance/identity-restoration (last visited Dec. 9, 2016).

identity fraud expense reimbursement.[138] In identity restoration insurance, a case worker is assigned to work with a lessee and assists the lessee in going through the restoration process in an effort to fix one's good name and credit.[139]

The identity fraud service reimburses a victim for preapproved covered expenses.[140] Both types of identity theft insurance would be helpful in reducing any damages that may come from a breach in the landlord's computer where a third party gains personal information about the lessee. The identity theft insurance may help in reducing the landlord's liability for certain damages. By having insurance to cover fraudulent charges, financial institutions may look to the insurance carrier to reimburse them instead of to the individual landlord who may not be able to fulfill a judgment against him or her. If the identity theft insurance carrier can show extreme negligence on the landlord's behalf in managing the lessee's personal information, the insurance carrier should be allowed to go after the landlord for a certain portion of the fraudulent expenses.

CONCLUSION

There are not many statutes or regulations that govern how a landlord who rents out a home, apartment, or individual room to a lessee can and should safeguard the lessee's personal information. Even with the few regulations that are out there, only a small handful of the regulations actually affect an individual landlord and his or her lessees. Many landlords do not have identity theft in mind when trying to rent out a unit or ensure a unit stays rented. This is why many documents containing sensitive information are not safeguarded properly after a rental application is received. If more regulations were in place, and landlords were made aware of such regulations and the liability that comes along with not adhering to them, there is a good chance identity theft for individual lessees would decrease.

There were a few suggestions given in this Note as to what landlords can do to limit the chances of their computer getting hacked and their lessee becoming a victim of identity theft. A landlord does not have to choose just one suggestion. Combining the requirement that a lessee obtain identity theft insurance and installing automatically updating security software on the landlord's computer increases the chances that a court would find that a landlord took reasonable steps in safeguarding the lessee's personal information. If a court was to find that a landlord was negligent or even reckless in the maintenance of a lessee's personal

138. *Id.*
139. *Id.*
140. *Id.*

information, there should be liability that attaches to the landlord regardless of whether or not the landlord was aware of any regulations and the consequences that follow.