The Geography of Medical Identity Theft
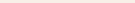
By Pam Dixon and John Emerson

WORLD **PRIVACY** FORUM

About This Report

This report is Part 1 of 3 reports the World Privacy Forum is publishing to share new research about the crime of medical identity theft, where it is occurring, when and how it happens, and impacts on victims of the crime. Part I of this report series is focused on the *where* of medical identity theft, and documents the distinct regional and state patterns of the crime suggested by the data as well as the growth patterns of medical identity theft across the United States.

This report was presented at the US Federal Trade Commission Workshop on Informational Injury December 12, 2017. Parts 2 and 3 of the series are forthcoming.

Brief Summary of Report

Medical identity theft has existed in various forms for decades, but it was in 2006 that World Privacy Forum published the first major report about the crime. The report called for medical data breach notification laws and more research about medical identity theft and its impacts. Since that time, medical data breach notification laws have been enacted, and other progress has been made, particularly in the quality of consumer complaint datasets gathered around identity theft, including medical forms of the crime.

This report uses new data arising from consumer medical identity theft complaint reporting and medical data breach reporting to analyze and document the geography of medical identity theft and its growth patterns. The report also discusses new aspects of consumer harm resulting from the crime that the data has brought to light.

Summary of Findings and Recommendations

This report finds that medical identity theft is growing overall in the United States, however, there's a catch. The consumer complaint data suggests that the crime is growing at different rates in different states and regions of the US, creating medical identity theft "hotspots."

Populous states such as California, Florida, Texas, New York, and to a lesser degree, Illinois, often have high consumer complaint counts, which can result from population effects. Based on data analysis of "rate per million" so as to equalize for population, strong additional patterns emerge from the complaint data. Notably, a large cluster of southeastern states emerge as a regional hotspot for medical identity theft, with steady

growth patterns. Medical identity theft hotspots have also occurred in a dispersed mix of less populous states.

In addition to documenting geographic and growth patterns, the complaint data also documented significant and heretofore largely unreported patterns of harm related to debt collection resulting from medical identity theft, including debt collections documented to be one to three years in duration.

The documentation of debt collection impacts on victims of medical identity theft is new information, and needs to be added to the understanding of how medical identity theft impacts victims of the crime. Although impacts and modalities will be discussed in detail in Part 3 of this report series, this report touches on this research as it represents a significant adjacent finding.

Key recommendations in the report include:

- The Department of Health and Human Services should facilitate the collection of follow up information from those affected by medical data breaches, specifically including data to document medical debt collection activity post-breach.
- Policymakers and law enforcement agencies should take regional and state hot spots suggested by the data into account when planning resources for medical identity theft deterrence, prevention, and remedies.
- Healthcare providers and related stakeholders need comprehensive risk assessments focused on preventing medical identity theft while protecting patient privacy. These risk assessments need to include specific plans for handling patient debt collection practices, and specific procedures that will prevent debt arising from medical identity theft to be passed to a collection agency.
- Patients, medical data breach victims, and other identity theft victims should be aware of states where medical identity theft is more active.
- The Consumer Financial Protection Bureau should monitor medical debt collection practices more closely and address abuses.

About the Authors

Pam Dixon is the founder and Executive Director of the World Privacy Forum. She is the author of eight books, hundreds of articles, and numerous privacy studies, including her landmark Medical Identity Theft study. She has testified before Congress on consumer privacy issues as well as before federal agencies. John Emerson is a creative technologist working at the intersection of digital design, data, and social change. His data visualizations for World Privacy Forum have ranged from US medical identity theft data to global identity datasets, among others.

About the World Privacy Forum

The World Privacy Forum is a non-profit public interest research and consumer education group that focuses on the research and analysis of privacy-related issues. Founded in 2003, the Forum publishes significant privacy research and policy studies on health privacy, privacy self-regulation, financial privacy and identity issues, biometrics, and data broker privacy practices among other issues. The *Patient's Guide to HIPAA* is a long-standing resource maintained at WPF. WPF members have testified before Congress regarding privacy issues, including health privacy, and have regularly contributed privacy expertise to agency-level workshops at the Federal Trade Commission, the FDA, and HHS. For more, see www.worldprivacyforum.org.

Table of Figures

The Geography of Medical Identity Theft
by Pam Dixon and John Emerson

I. Introduction

Medical identity theft is growing, and this growth is emerging in distinct geographic patterns that hold peril and promise. Peril, because people living in some regions in the United States are far more likely to become victims of medical identity theft. Promise, because knowing the geographic patterns of the crime and quickly detecting geographic shifts in the crime can assist timely detection of the crime, direct help for victims, and potentially increase the possibility of prevention of the crime.
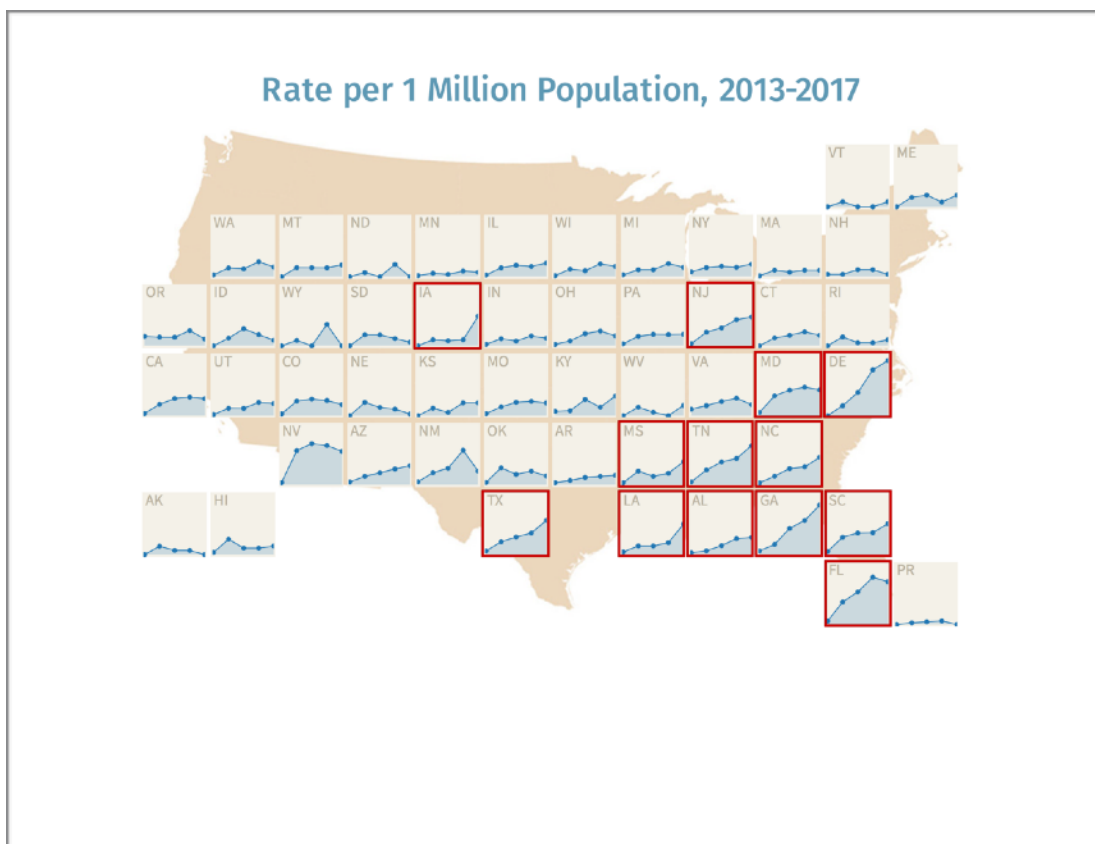

Figure 1: Overview of consumer complaints regarding medical identity theft issues, from 2013 - 2017, with regional and state-level growth hot spots highlighted. Data visualization: John Emerson.

Of all the identity crimes, medical identity theft is a crime that has thus far resisted detection, prevention, and remediation efforts. This crime can cause significant and often enduring harms to its victims, and it has left a trail of victims who have suffered deeply. The World Privacy Forum (WPF) first documented the breadth of harms of medical identity theft in a 2006 report, which was the first major report to be published about this crime. In this report, WPF coined the term "medical identity theft" and defined a crime that was in its essence, a subset of healthcare fraud. Today, the definition still holds true:

> Medical identity theft occurs when someone uses a person's name and sometimes other parts of their identity — such as insurance information — without the person's knowledge or consent to obtain medical services or goods, or uses the person's identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim's name.[1]

Medical forms of identity theft are difficult to fix after the fact, because victims have limited rights and recourses. In WPF's first report, research documented that medical identity theft typically leaves a trail of falsified information in medical records that can plague victims' medical and financial lives for years. This is still true, and is a root harm of the crime. The report also documented various insurance and debt collection issues victims frequently face. In the intervening years since WPF's initial publication about medical identity theft, further research has documented how these and additional harms develop over sometimes long periods of time. The consequences of medical identity theft still remain among the most severe of all identity crimes, and time has not lessened the severity of consequences victims may experience. Complications from medical identity theft can endure for years.

Research for the current report uncovered new aspects of harms victims of medical identity theft can experience.

Medical identity theft victims can experience:

• Changes to their health care records, most often the addition of falsified information, through improper billing activity or activity by imposters. These changes can then affect the healthcare a person receives if the errors are not caught and corrected.
• Significant bills for medical goods and services they neither sought nor received.
• Issues with insurance, co-pays, and insurance caps.

---

[1] Pam Dixon, (author) Robert Gellman, (ed.) *Medical Identity Theft: The information crime that can kill you,* World Privacy Forum, May 2006. https://www.worldprivacyforum.org/2006/05/report-medical-identity-theft-the-information-crime-that-can-kill-you/.

- Long-term credit problems based on problems with debt collectors reporting debt due to identity theft.
- Serious life consequences resulting from the crime; for example, victims have been falsely accused of being drug users based on falsified entries to their medical files; victims have had their children removed from them due to medical activities of the imposter; victims have been denied jobs due to incorrect information placed in their health files due to the crime, in the aftermath of the crime.
- Data gathered in the last 5 years and data analyzed for this report sheds new facts and light on the seriousness of debt collection problems for victims. Victims can experience long term problems with aggressive medical debt collection arising from debt that does not belong to them. As a result of improper or even potentially fraudulent medical debt reporting, some victims may not qualify for mortgage or other loans and may experience other financial impacts.
- Phantom medical debt collection based on medical billing or other identity information is an additional modality of harm.
- Sales of medical debt arising from identity theft can perpetuate a victim's debt collection and credit problems, through no fault of their own.
- Victims still experience a general lack of ability to cure the full range of problems medical identity theft brings, even over the course of years for some victims.

Since 2006, WPF has continued to study medical forms of identity theft by conducting field research in hospitals, interviews across the healthcare spectrum and associated stakeholders, and working directly with victims of the crime. WPF has also sought consumer self-reporting data from both the US Federal Trade Commission (FTC) and the Consumer Financial Protection Bureau (CFPB) as well as medical data breach reports from the US Department of Health and Human Services (HHS) data breach portal.[2] The preponderance of the data gathered and analyzed in these efforts consistently shows new patterns in medical identity theft that are significant and need to be brought forward.

This report is Part 1 of three reports that discuss WPF's new research and findings regarding medical identity theft. This report focuses on the geographical patterns of medical identity theft, what those patterns tell us, and how best to use that information. Some of the data analyzed for this report has also shed new understanding of the debt collection activities that victims of medical identity theft experience.

(Part 2 of the forthcoming medical identity theft report series focuses on biometric identity, and biometric identity theft, in the healthcare context. Part 3 is focused on an updated analysis of modalities of the crime, impacts, and potential solutions.)

---

[2] US Department of Health and Human Services, Office for Civil Rights, Breach Portal. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

Findings:

- Consumer complaint data suggests that medical identity theft is growing overall in the United States.
- Consumer complaint data suggests that medical identity theft is growing at detectably different rates in different regions and states in the US, creating medical identity theft "hotspots."
- Consumer complaint data suggests that individual states can show unpredictable spikes in activity and drops in activity.
- Consumer complaint data suggests a large cluster of southeastern states are currently a significant regional hotspot for medical identity theft, with steady growth patterns.
- The consumer complaint data analyzed also documented significant heretofore largely undocumented patterns of harm related to aggressive debt collection resulting from medical identity theft, including problems with debt collection documented to be one to three years in duration. This is new information, and needs to be added to the understanding of the crime's impacts on victims.

II. Discussion

Medical identity theft is growing, and medical identity theft grows in distinct, discernible patterns. While it may seem obvious to the observer that this crime is likely increasing, it has been difficult to document satisfactorily. It has been even more difficult to document the geographic distribution of the crime due to lack of consistent patterns of national data over time. The importance of documentation of the growth and distribution of the crime is particularly important because both have implications for consumer risk, and for methods used to detect and treat the crime, and ultimately, it could help in prevention efforts.

New Data and Datasets

In WPF's 2006 report, there were datasets that described multiple aspects of identity theft patterning and healthcare fraud, but at the time, acquiring nationally reported instances of medical identity theft was not a simple matter to acquire, mainly because people had not been collecting data around that issue. Since 2006, several important new datasets with potential to shed light on the crime have been collected and made public. This report is focused on the analysis and visualization of these datasets, which are from the FTC, the CFPB, and the US Department of Health and Human Services. The datasets include:

FTC Consumer Sentinel Data

The FTC dataset WPF references in this report ranges from 2003-2016 and was acquired through multiple Freedom of Information Act requests from 2006 to 2016 to the FTC Consumer Sentinel Database.[3] Filters for the data included the keywords of "Medical identity theft" "Medical ID theft" "Insurance fraud" "Medical ID fraud" "Medical identity fraud" and "Medical record theft." WPF did not have direct access to query the dataset, the queries were run by the FTC and sent to WPF. The full dataset of FTC FOIAs WPF acquired is in excess of 20,000 consumer complaints. The dataset WPF used for the focused analysis of city-level data included in this report included 1,521 total complaints.

CFPB Consumer Complaint Database Data

CFPB maintains a robust Consumer Complaint Database.[4] The CFPB posts complaints after the company responds, or after 15 days, whichever comes first. We analyzed CFPB consumer complaint data from 2013-2017. We downloaded and worked with the entire dataset, and tested a variety of filters to focus the results on medical identity theft complaints. The filters for the final datasets analyzed in this report include: Debt is not mine, Debt resulted from identity theft, Debt is not yours, Debt was result of identity theft, Medical, Medical debt. WPF was able to query the database directly and apply filers by layers. There are 6,939 total complaints in the CFPB data used in this report. Of these, 6,891 have state codes listed. AE (a US military base), AP (a US military base), AS (American Samoa), are not displayed on the cartogram. Washington DC statistics are are displayed on the Dot Matrix analysis.

HHS Office for Civil Rights Breach Portal Data

HHS has maintained a Medical Data Breach Portal and database since 2009.[5] We downloaded and analyzed All data available, from the date ranges of 2009-2016.

The CFPB datasets and the HHS datasets are updated as living databases, with minimal lag times between complaint and data entry. These databases are made public and are readily searchable. These databases have provided significant insight into consumer data trends.

---

[3] FTC Complaint Assistant, (Consumer Sentinel Database is generally non-public). https://www.ftccomplaintassistant.gov/?utm_source=takeaction#crnt&panel1-1. Data is from FOIAs from World Privacy Forum dated 2006 through 2016.

[4] Consumer Financial Protection Bureau, Consumer Complaint Database Dataset. https://www.consumerfinance.gov/data-research/consumer-complaints/

[5] Department of Health and Human Services, Office for Civil Rights, Breach Portal, Database available on page. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf.

Data Quality and Methodology

The data WPF analyzed for this report allows for views inside consumer trends that were not possible even as recently as a few years ago. The data is exciting, but it is still not perfect — self-reported medical identity theft data has inherent shortcomings.

First, people who are victims of medical identity theft may not know they are victims of the crime for weeks, months, or even years. This creates a lag time in reporting. It is a well-known feature of medical identity theft that it is a crime that hides itself well. Medical identity theft is a form of health care fraud, which, like other kinds of white-collar fraud, is not a self-revealing crime. Malcolm Sparrow's seminal work in this area contains a thorough discussion of this point.[6]

Second, some people may *never* learn they are victims, which creates underreporting. There is not a formula yet for determining how much medical identity theft is underreported. We do not know if it is underreported by 5 percent, 15 percent, 50 percent, or more. This data does not reveal a full denominator of all known victims. Rather, it shows us a subset of victims who had, in some way, learned of the crime. This needs to be kept in mind when reading the data.

Third, those who know they are victims may not know about reporting a problem at the FTC or CFPB, or they may not choose to make such a report. This too, contributes to underreporting.

Fourth, in self-reported datasets there can be errors in the data, for example, when a person makes two reports instead of just one. There can also be other influences on who reports, which may not be apparent to an observer of the data. So this data should be understood in this context. It is not wise to derive sharply-drawn conclusions from a body of self-reported complaint data.

However, understanding the limitations of self-reported complaint data, it is also true that a strong national system for consumer reporting has created a national footprint of patterns that can be studied over time, and given enough time, the patterns can be relied on with more trust.

WPF has now collected robust enough data over time to determine that even if the data have errors, even if the data are underreported, there is now enough data to see discernible geographic and growth trends in the crime.

---

[6] See discussion in Malcolm K. Sparrow, License to Steal: How Fraud Bleeds America's Health Care System at 120 (Westview Press, 2000).

III. Data Visualizations and Analysis, 2009-2017

This section of the report contains data visualizations and analysis based on the key data sets described in Part II of this report.

Medical Identity Theft Mapped By City:
US Federal Trade Commission City-Level Data, 2008-2009

WPF has mapped a full year of medical identity theft consumer complaints by city, state, and zip code.

Background of the city-level data analysis

To create this analysis and data visualization, WPF requested and received in excess of 20 years of Federal Trade Commission consumer complaint data regarding medical identity theft. The dates for the complaint data range from 1992 to 2016. WPF began requesting medical identity theft data from the Federal Trade Commission in 2006 via Freedom of Information Act requests, some of which were lengthy. Since 1992 to 2016, the FTC has recorded that in excess of 20,000 individuals have filed complaints specifically concerning medical identity theft. For the FTC, an agency that does not handle medical issues, this represents a high number.

In order to attempt to understand geographic patterns in the numbers, WPF requested a city-by-city breakdown of a portion of the data, correlated with zip codes so that identical city names could be disambiguated.

WPF created a visualized data snapshot of this detailed city-level complaint information for a date segment that extended from 2008-2009. This data snapshot is interactive on the World Privacy Forum website. This report includes a static image of the visualized dataset.

Each red dot on the map represents a consumer complaint tied to a specific city. The map is configured to show simple count only, by city. The larger the dot, the more complaints consumers living in those cities made to the FTC.
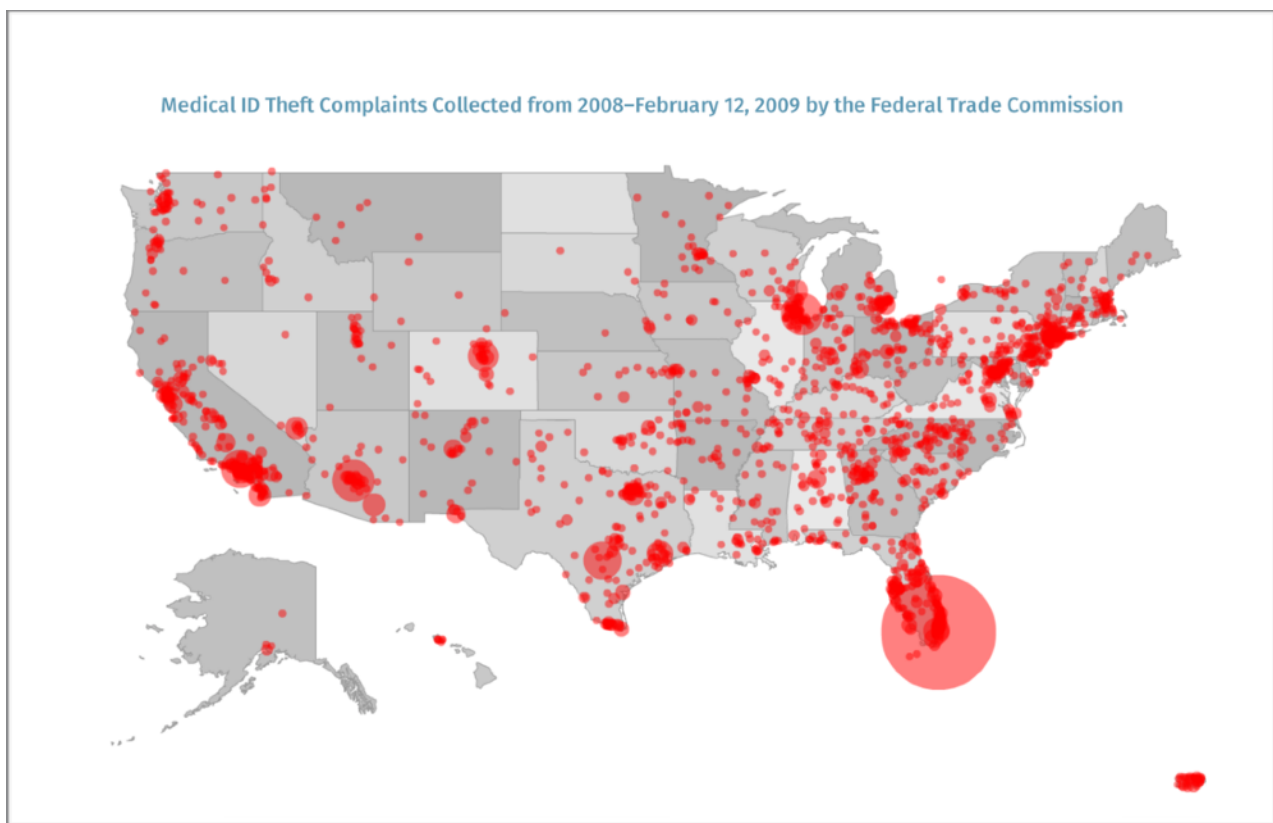
Figure 2: FTC city-level Consumer Sentinel medical identity theft complaints, 2008-2009. Data visualization John Emerson. Interactive version available at https://www.worldprivacyforum.org/2011/08/medicalidentitytheft-map/.

Analysis: What the city-level data tells us

This data visualization of the city-level complaints reveals overall patterning of medical identity theft with significant concentrations in Northern and Southern California, Phoenix, Arizona, Chicago Illinois, many cities throughout Florida, but especially cities in South Florida, and a strong distribution of complaints throughout the eastern seaboard.

Some dispersed city-level hotspots appear in Denver, Colorado, the Vancouver-Portland metro area, Seattle, and the largest cities in Texas. Of the states, North Dakota had no complaints for this time frame.

This map was created using simple counts by city, and was not adjusted to rate per million, as it was tied directly to individual instances of medical identity theft in cities,

not in states, making that estimation difficult to achieve to a sufficient degree of accuracy. What this means is that areas with generally higher populations will show more complaints. This map is best used to track city-level medical identity theft concerns.

This map represents the earliest snapshot WPF is aware of that documents consumer medical identity theft complaints at the city level.

Medical Identity Theft Complaint Data Mapped by State: Consumer Financial Protection Bureau Consumer Complaint Data, 2013-2017

WPF has mapped five years of medical identity theft-related complaints consumers made to the CFPB. The CFPB data is mapped at the state level in a series of data visualizations over the five year period.

Background of this analysis

WPF has mapped the CFPB consumer complaint data at the state level two ways.

Count of Reports analysis

First, the data is visualized by simple count, called Count of Reports. A count of reports shows the number of total complaints in each state. A simple count number will reflect the influence of large population centers. For example, raw counts of consumer complaints typically show more complaints coming from highly populous areas such as California, New York, and Texas. This does not always mean the actual rate of medical identity theft is higher in those locations. It does usually mean there are overall higher volume of cases in those areas with higher populations.

Rate per 1 million analysis

Second, the data is visualized by rate per 1 million. Rate per 1 million allows a view of the data that is not skewed by population size. Therefore, the data will not automatically show the large cities as the hotspots of medical identity theft by virtue of sheer population volume. Instead, the data shows where the hotspots are occurring across all population sizes by rate of incidence.

The data visualizations include overviews of combined years, as well as year-by-year analysis.

The dataset analyzed includes data from 2013-Dec. 4, 2017. Note that the 2017 numbers will be updated in January, 2018.

The CFPB dataset visualizations are presented in this order:

Dot Matrix Side-by-Side Comparison and Overview, 2013-2017

Year-by-Year progressions:

       2013, count of reports
       2013, rate per 1 million

       2014, count of reports
       2014, rate per 1 million

       2015 count of reports
       2015, rate per 1 million

       2016, count of reports
       2016, rate per 1 million

       2017, count of reports
       2017, rate per 1 million

Cartogram Overview, count of reports 2013-2017

Cartogram Overview, rate per 1 million 2013-2017

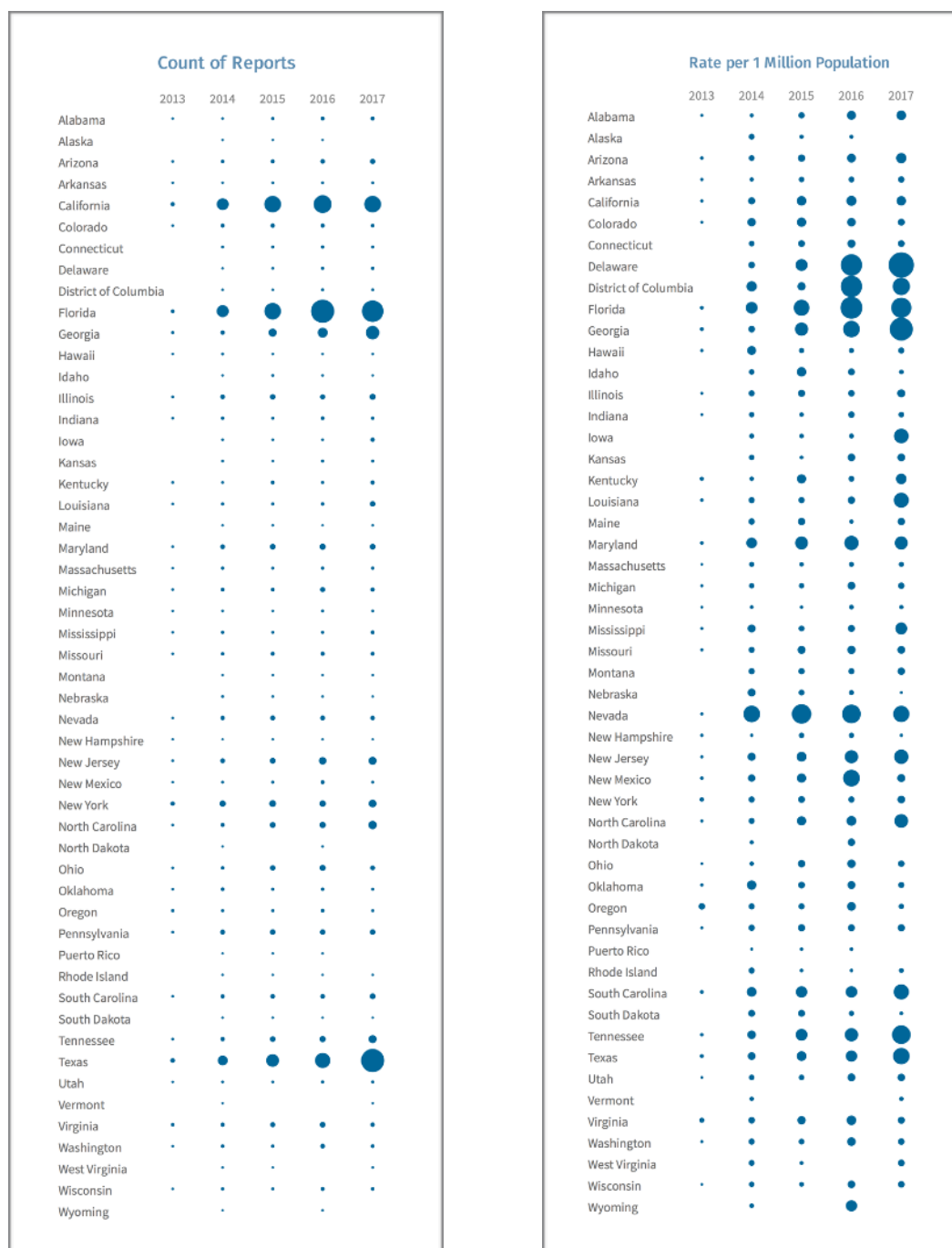**Dot Matrix Data Visualization of CFPB Data, Overview 2013-2017**

Figure 3: Left side: Count of Reports from 2013-2017. Each dot represents the volume of consumer medical identity theft-related complaints based on number of complaints only. Figure 3: Right side: Reports by rate per 1 million population. Each dot represents the rate of consumer complaints per 1 million. Data visualization: John Emerson

Analysis: What the Dot Matrix data visualization tells us

In Figure 3, left side, the Count of Reports dot matrix shows California, Florida, Texas, Illinois, Maryland, New Jersey, and New York as complaint hot spots. These results show that these states have the most overall complaints by simple count. It is a fair generalization to say that these states have more overall activity. But the generalizations must be tempered by acknowledging the potential action of population density.

In Figure 3, right side, the Rate Per 1 Million dot matrix, the numbers suggest a different — and important story. This dot matrix reveals the deeper pattern of medical identity theft hot spots over the five year period, adjusted to equalize the impact of population density. In this analysis, a more complex picture emerges of the distribution of medical identity theft complaints.

Florida, Georgia, and Texas still show up as complaint hot spots. But Tennessee increases in prominence, as does Delaware, Nevada, South Carolina, and during one year, New Mexico. The data suggests a stronger pattern of overall growth, with an expression of particular strength in many of the southeastern states.

Year -By-Year Progressions
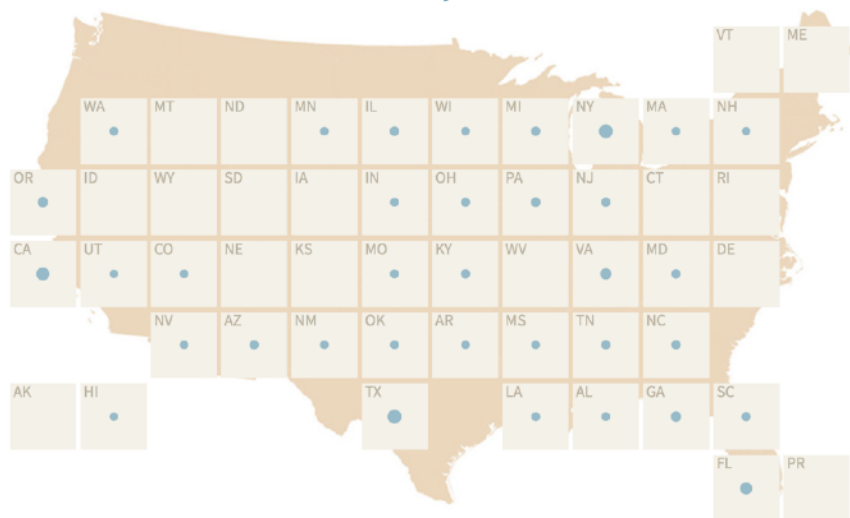

Analysis: What the 2013 data tells us

In 2013, the consumer complaint data was sparse, even for California. Some states had no complaint data — Alaska, Idaho, Montana, North Dakota, Wyoming, South Dakota, Iowa, Nebraska, Kansas, Connecticut, Rhode Island, Vermont, Maine, Delaware and Puerto Rico did not register complaints.

A comparison between the count of report and the rate per million (below, Figure 5) shows that only Oregon had a slight increase in the rate. But it was not a significant increase, and overall, the rates show sparsity.
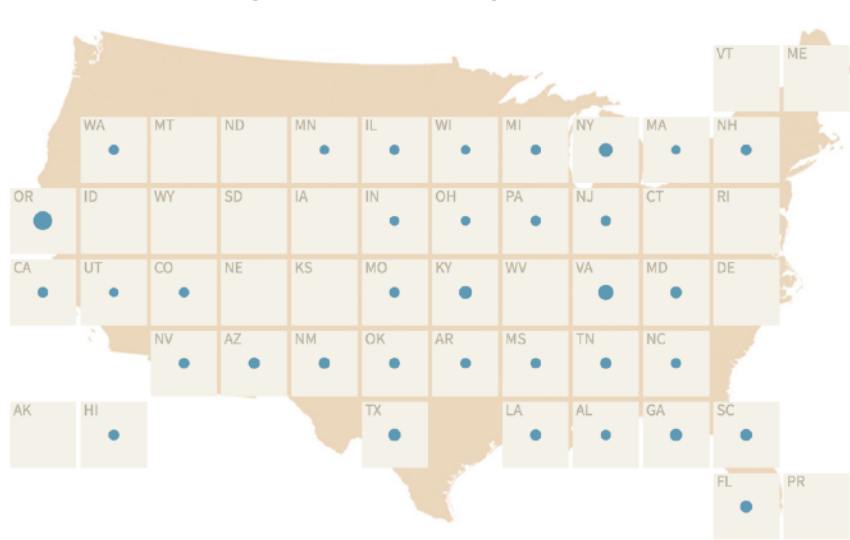
Figure 4: Next page, top. Count of Reports from 2013, below. Each dot represents the volume of consumer medical identity theft-related complaints based on number of complaints only. Data visualization: John Emerson.

Figure 5: Next page, bottom. Rate per 1 Million Population, 2013. Each dot represents the rate of consumer medical identity theft-related complaints adjusted for population density. Data visualization: John Emerson.

Count of Reports, 2013

Rate per 1 Million Population, 2013

Analysis: What the 2014 data tells us

In 2014, the count of reports data reveals that all states registered complaints. California, Texas, Florida, and to a lesser degree, New York emerge as high-volume medical identity theft hotspots.

The rate per 1 million data analysis reveals that for their respective sizes, the states of Nevada, Florida, South Carolina, and Maryland showed signs of increased activity.
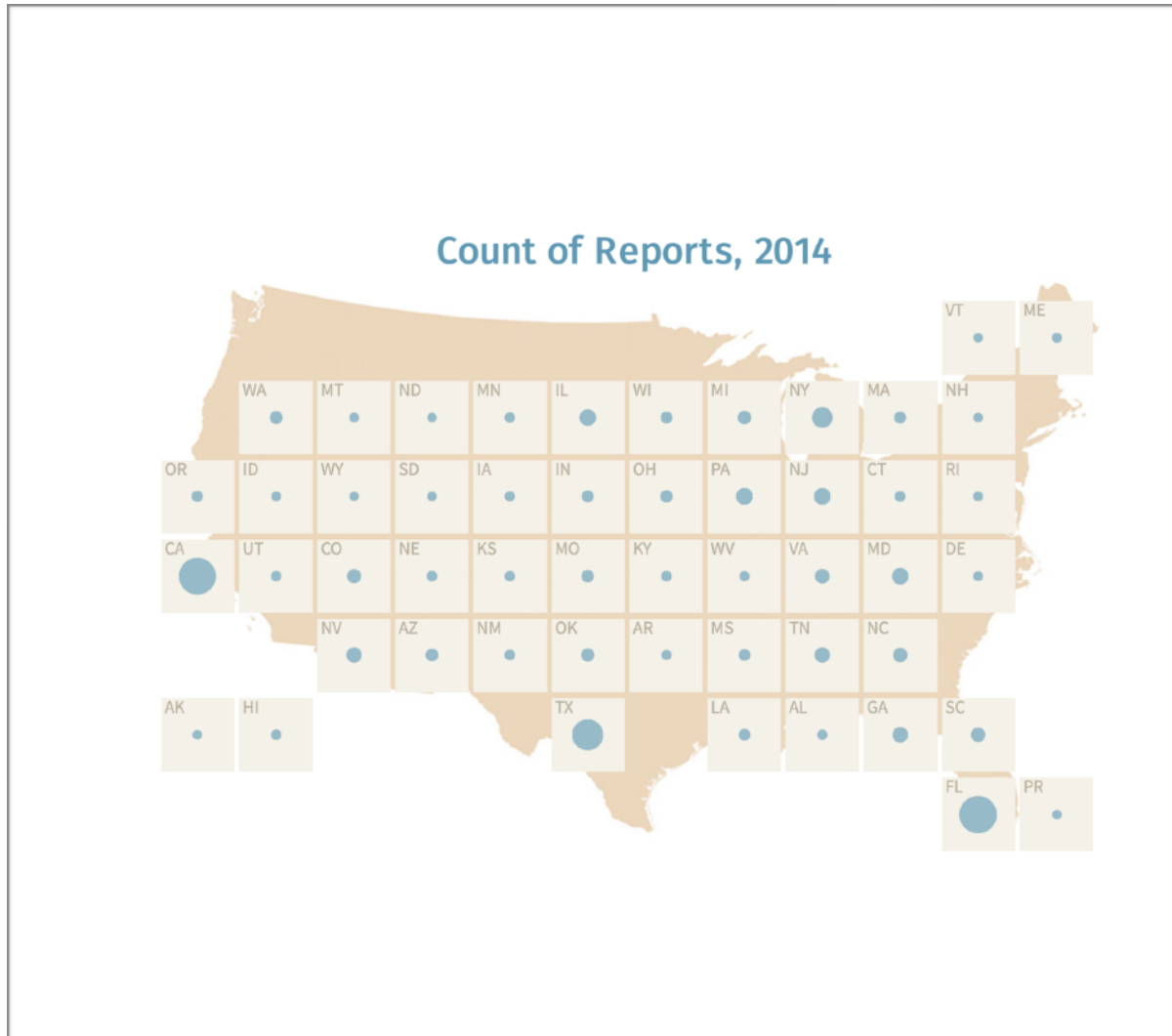

Figure 6: Count of Reports from 2014. Each dot represents the volume of consumer medical identity theft-related complaints based on number of complaints only. Data visualization: John Emerson.
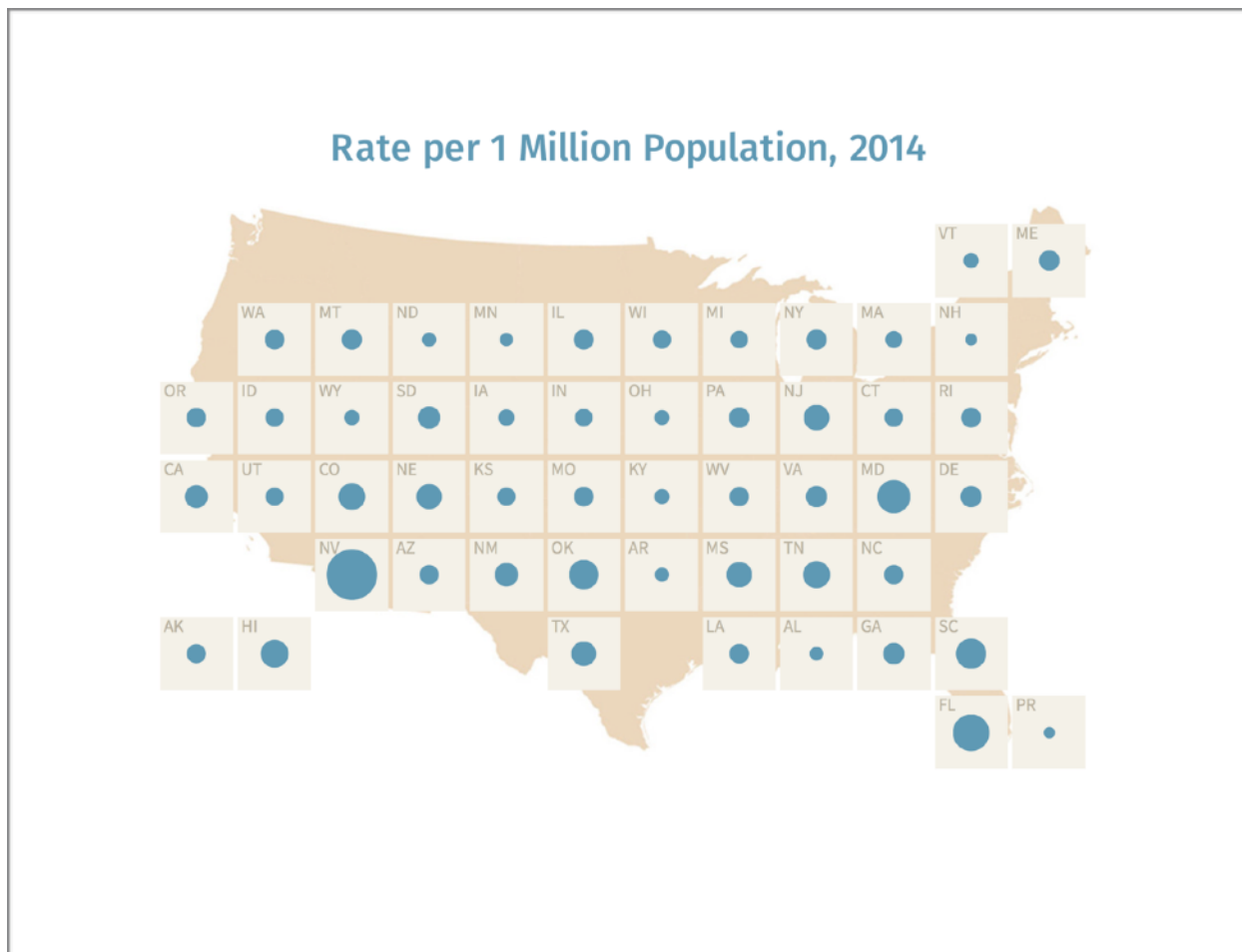
Figure 7: Rate per 1 Million Population, 2014. Each dot represents the rate of consumer medical identity theft-related complaints adjusted for population density. Data visualization: John Emerson.

Analysis: What the 2015 data tells us

In 2015, the count of reports map shows California, Texas, and Florida dominating the count totals, with Georgia showing increases. Vermont, North Dakota, and Wyoming do not show any complaints.

The rate per 1 million analysis shows Nevada's continued growth pattern, with new momentum from Idaho, and a swath of the southeastern states begin to show a marked pattern of growth activity.
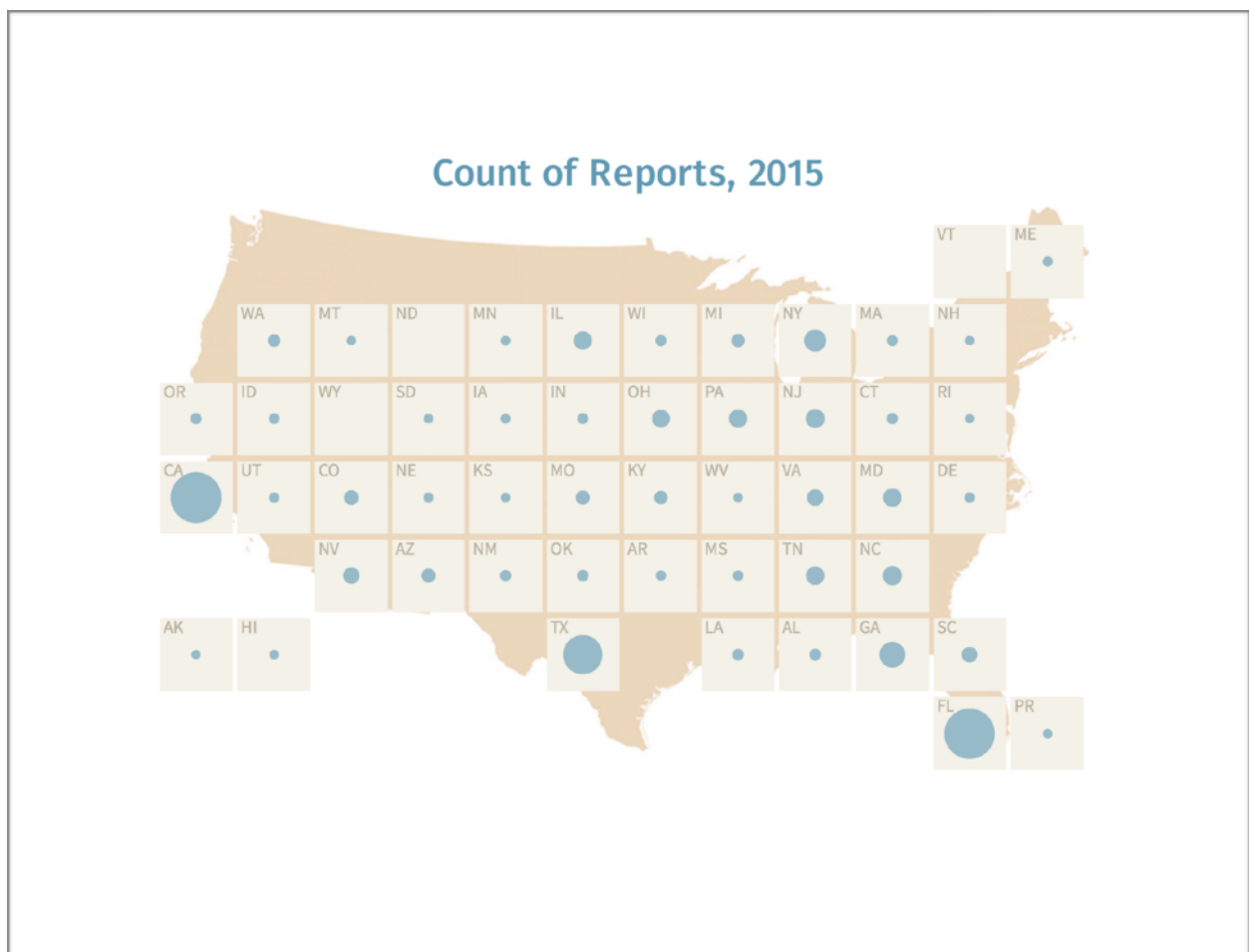

Figure 8: Count of Reports from 2015. Each dot represents the volume of consumer medical identity theft-related complaints based on number of complaints only. Data visualization: John Emerson.
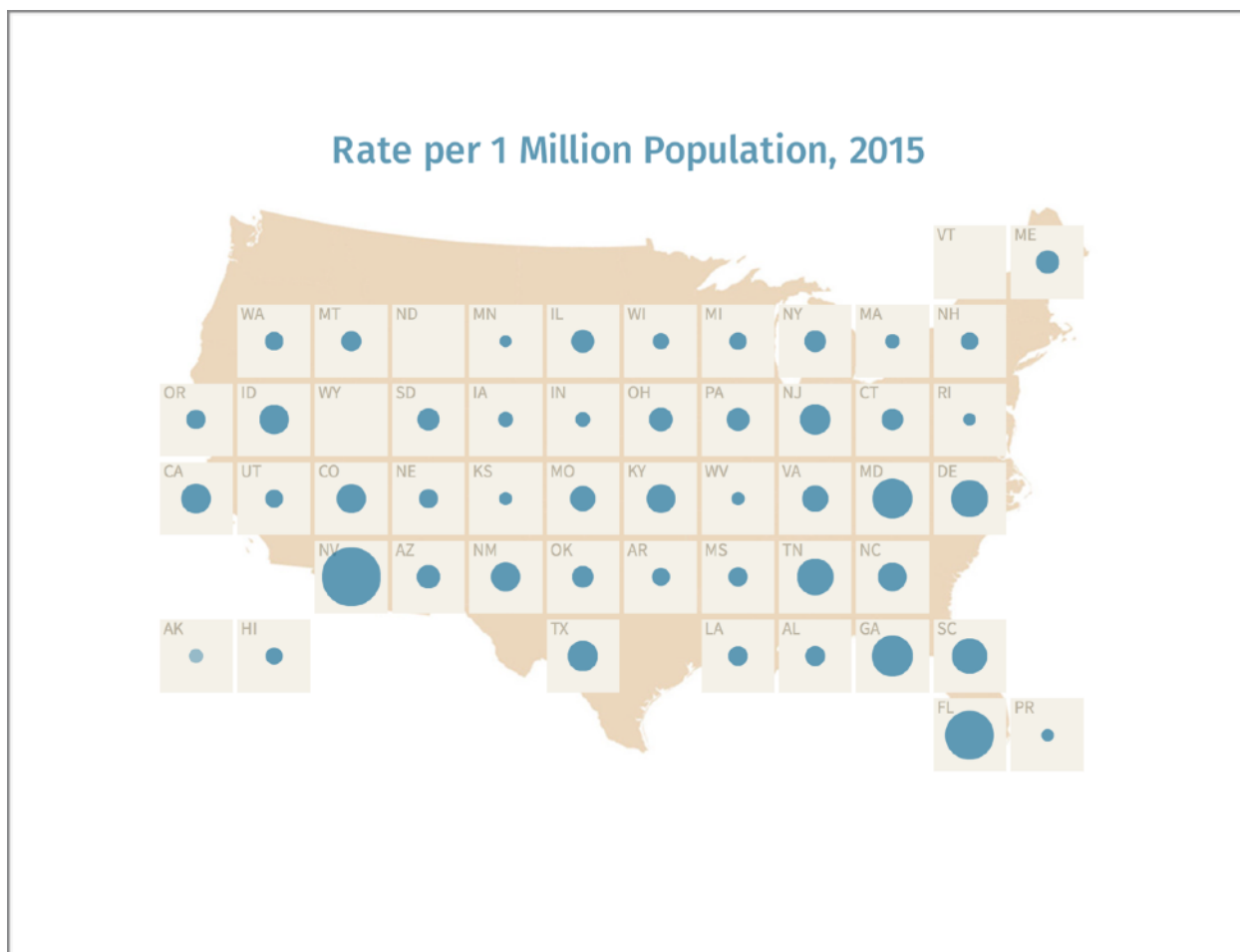
Figure 9: Rate per 1 Million Population, 2015. Each dot represents the rate of consumer medical identity theft-related complaints adjusted for population density. Data visualization: John Emerson.

Analysis: What the 2016 data tells us

In 2016 the count of reports map begins to show patterns of increased activity in the Southeast and upper midwest, with California, Texas, Georgia, and Florida still showing high counts.

In the rate per 1 million map, the hints of a developing hot spot in the general southeastern region grow to a full-fledged trend. Several individual states continue to

show fluctuations. Generally, though, the trend is toward growth. West Virginia and Vermont are exceptions, and do not report any complaints.
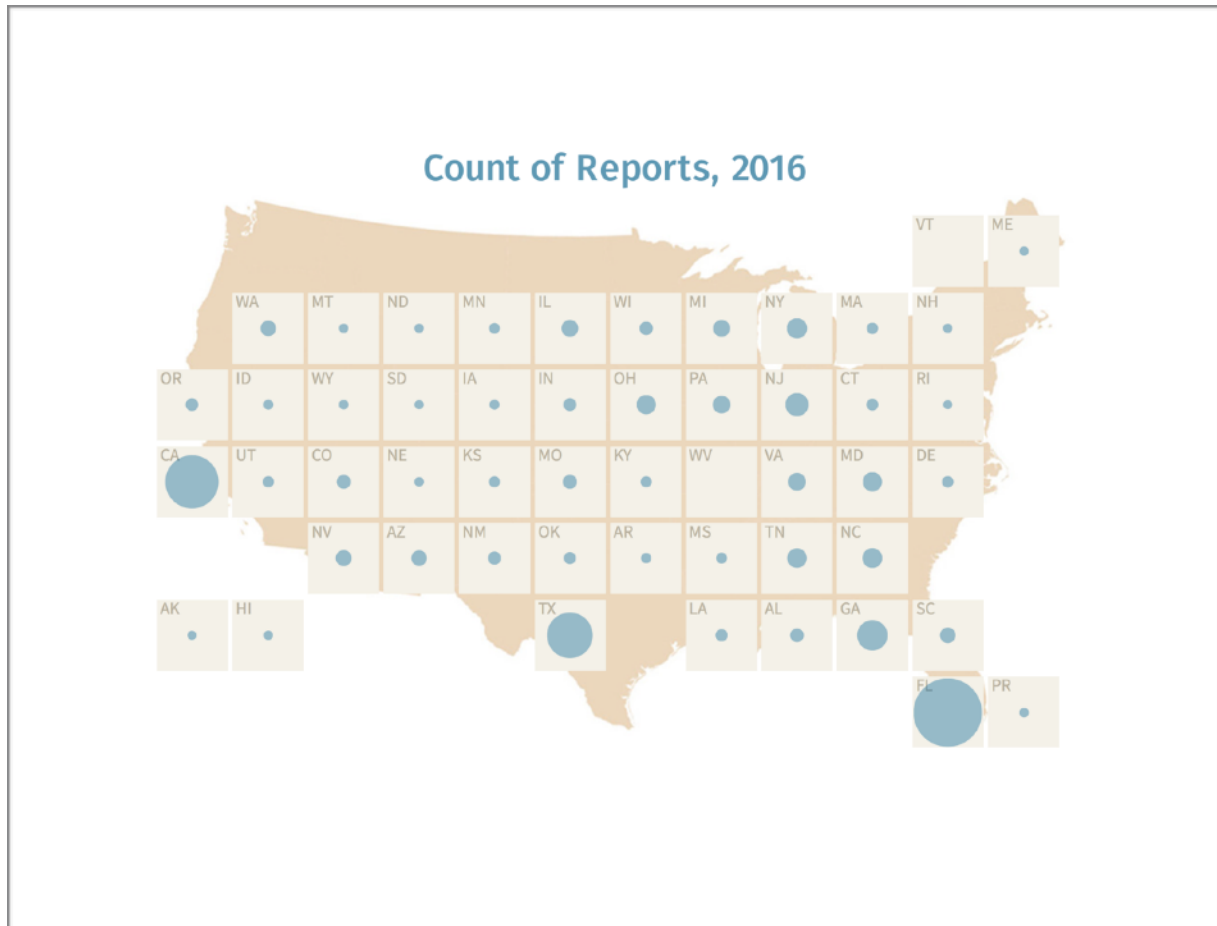

Figure 10: Count of Reports from 2016. Each dot represents the volume of consumer medical identity theft-related complaints based on number of complaints only. Data visualization: John Emerson.

Figure 11: Rate per 1 Million Population, 2016. Each dot represents the rate of consumer medical identity theft-related complaints adjusted for population density. Data visualization: John Emerson.

Analysis: What the 2017 data tells us

In 2017, the count of reports shows Nevada, Wyoming, Alaska, and Puerto Rico as having no complaints. But the trends of California, Texas, Georgia, and Florida showing high counts continues.

The most dramatic result is viewable in the 2017 rate per 1 million map. This map shows pronounced growth in activity in the southeastern region, with individual hotspots of Nevada, Iowa, Texas, and in states edging up the eastern seaboard.

Figure 12: Count of Reports from 2017. Each dot represents the volume of consumer medical identity theft-related complaints based on number of complaints only. Data visualization: John Emerson.
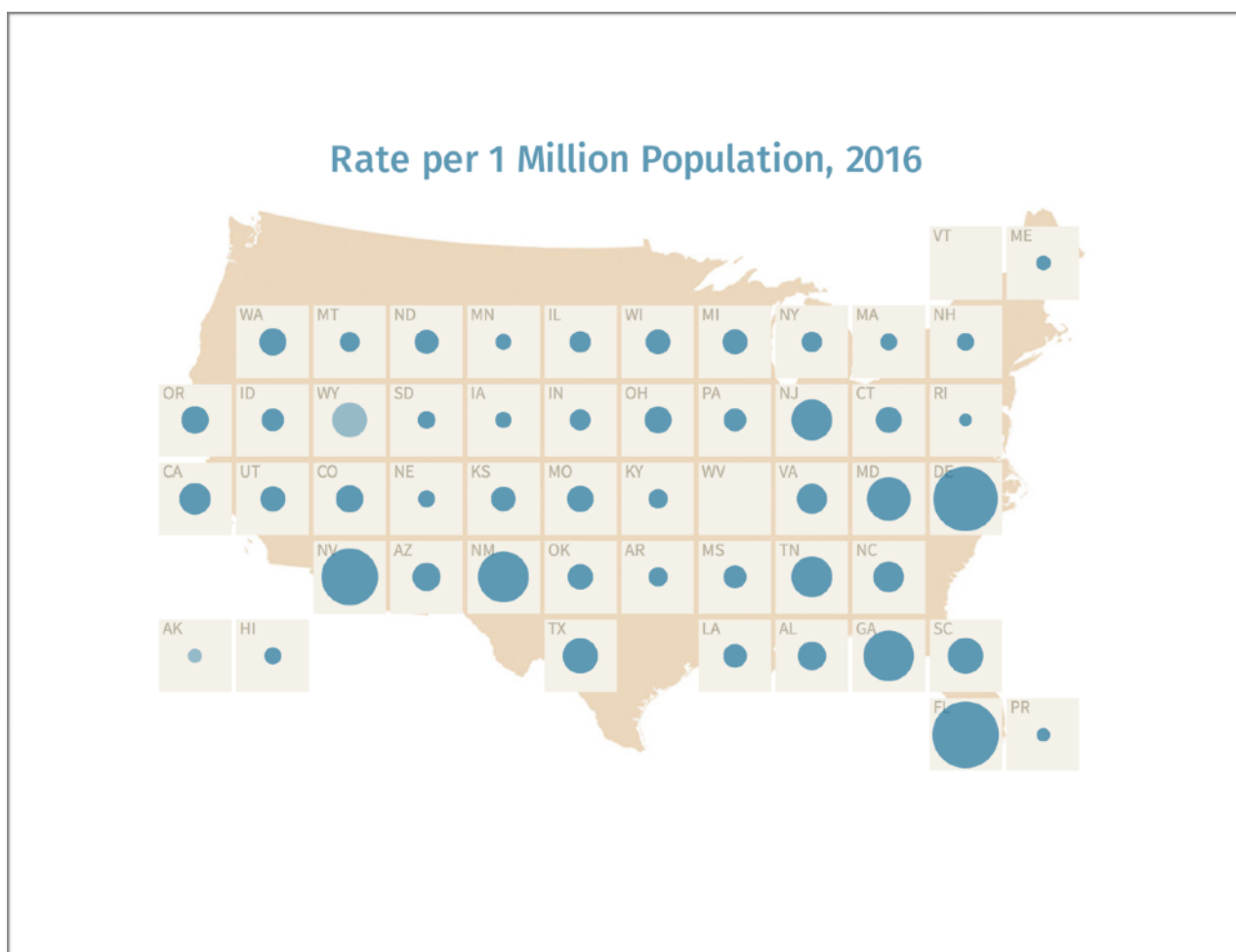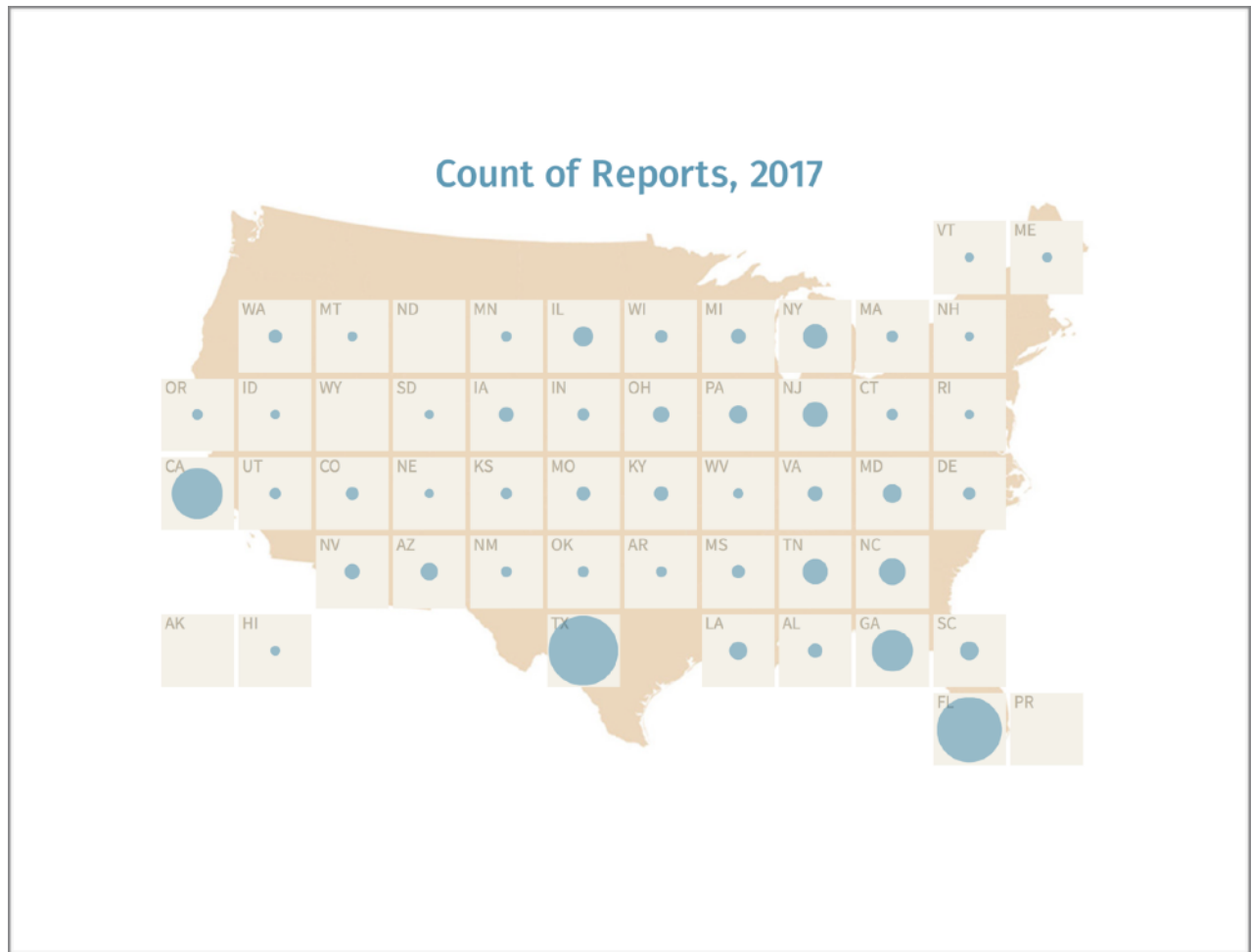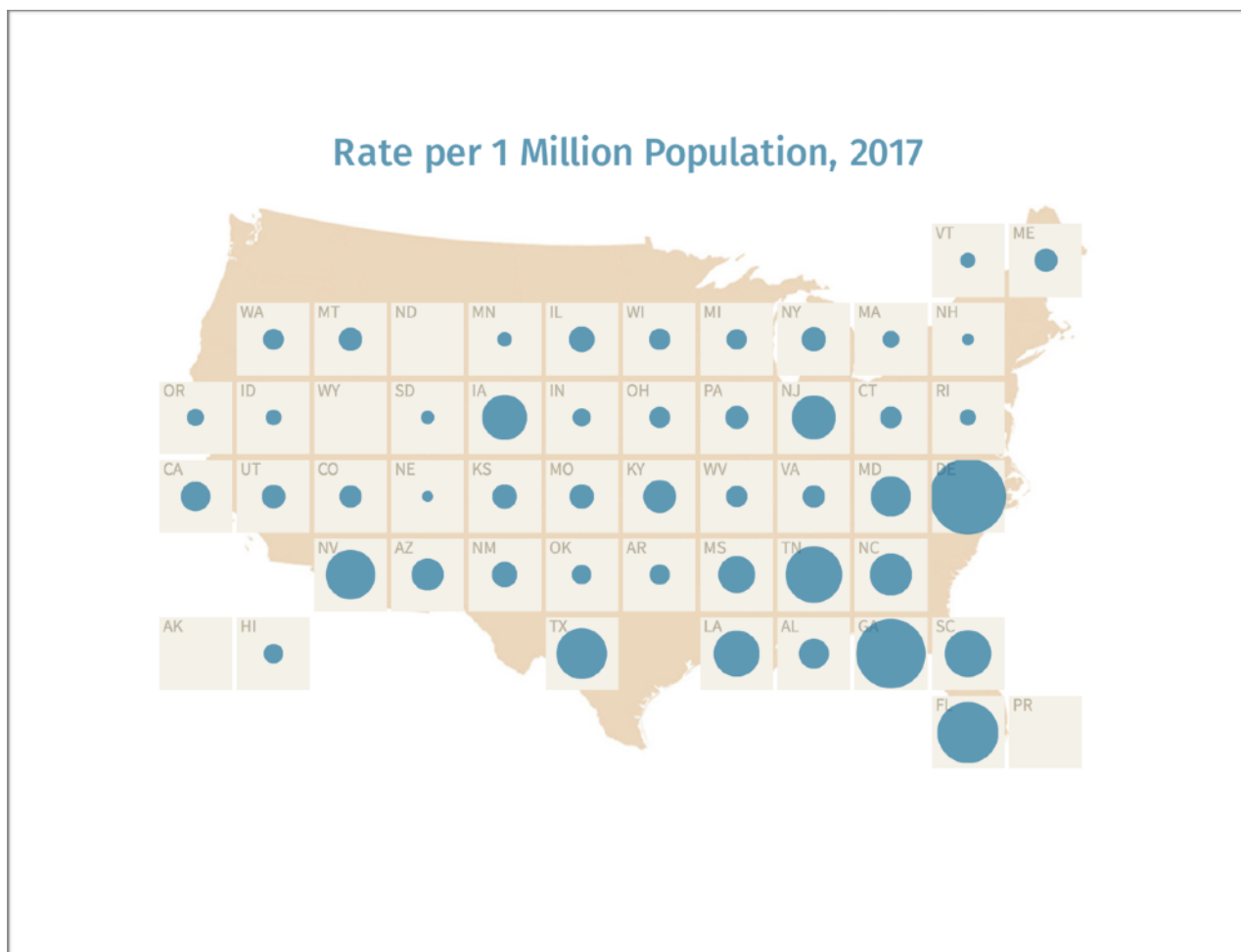
Figure 13: Rate per 1 Million Population, 2017. Each dot represents the rate of consumer medical identity theft-related complaints adjusted for population density. Data visualization: John Emerson.

Analysis: What the 2013-2017 composite data visualization tells us

The 2013-2017 comparison maps of consumer complaints gives an overview of the years, and is simply a more compact view of the data. Note, however, the visualization of the data for Florida. In the FTC data and in the CFPB data, Florida has become a hotspot both in volume and in rate. Overall, the data suggest strong regional growth trends. In the rate per 1 million map, distinct growth patterns are present.
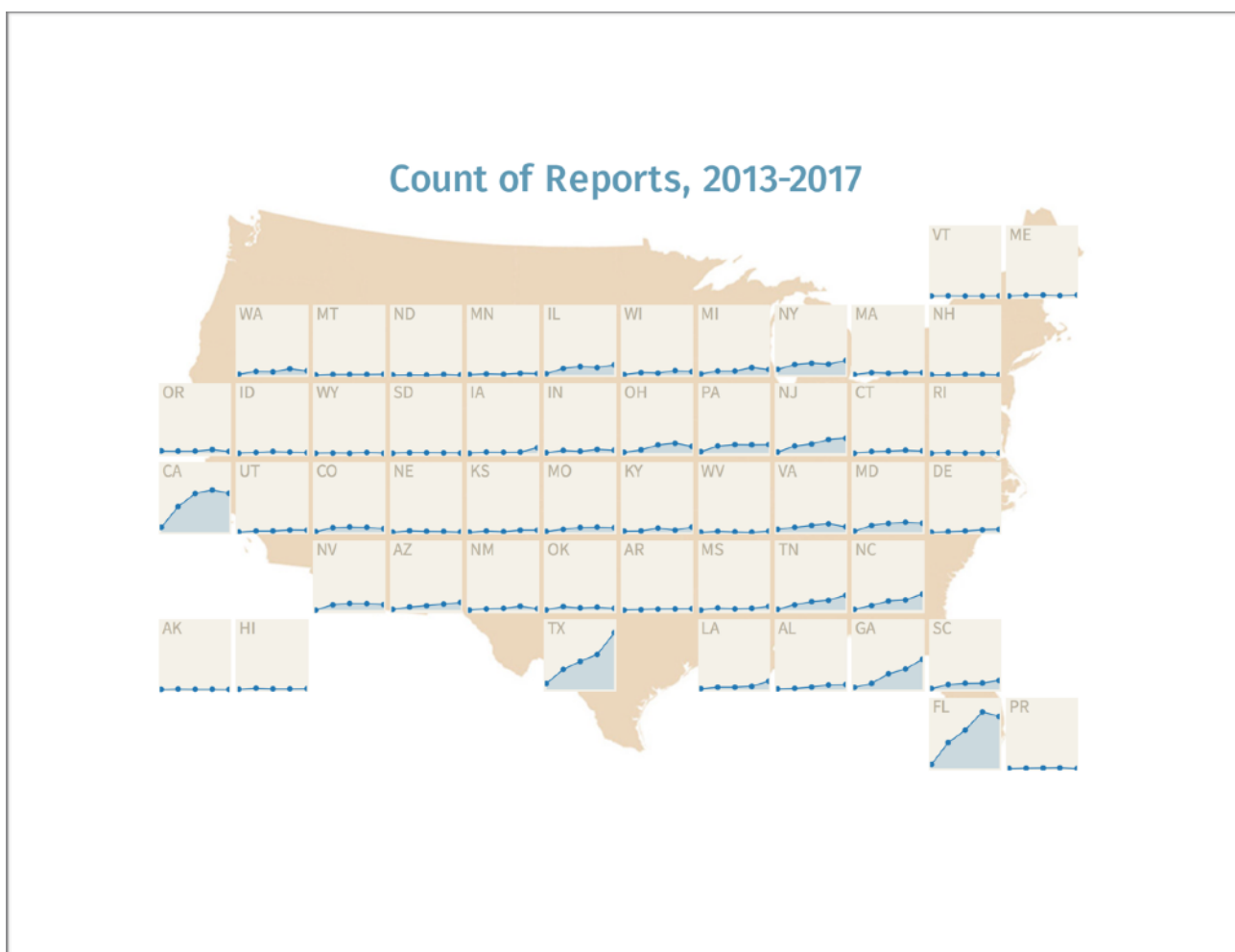
Figure 14: Count of Reports from 2013-2017. Each dot represents one year, and the line of dots in each box represents the overall volume and change in consumer medical identity theft-related complaints based on number of complaints only. Data visualization: John Emerson.
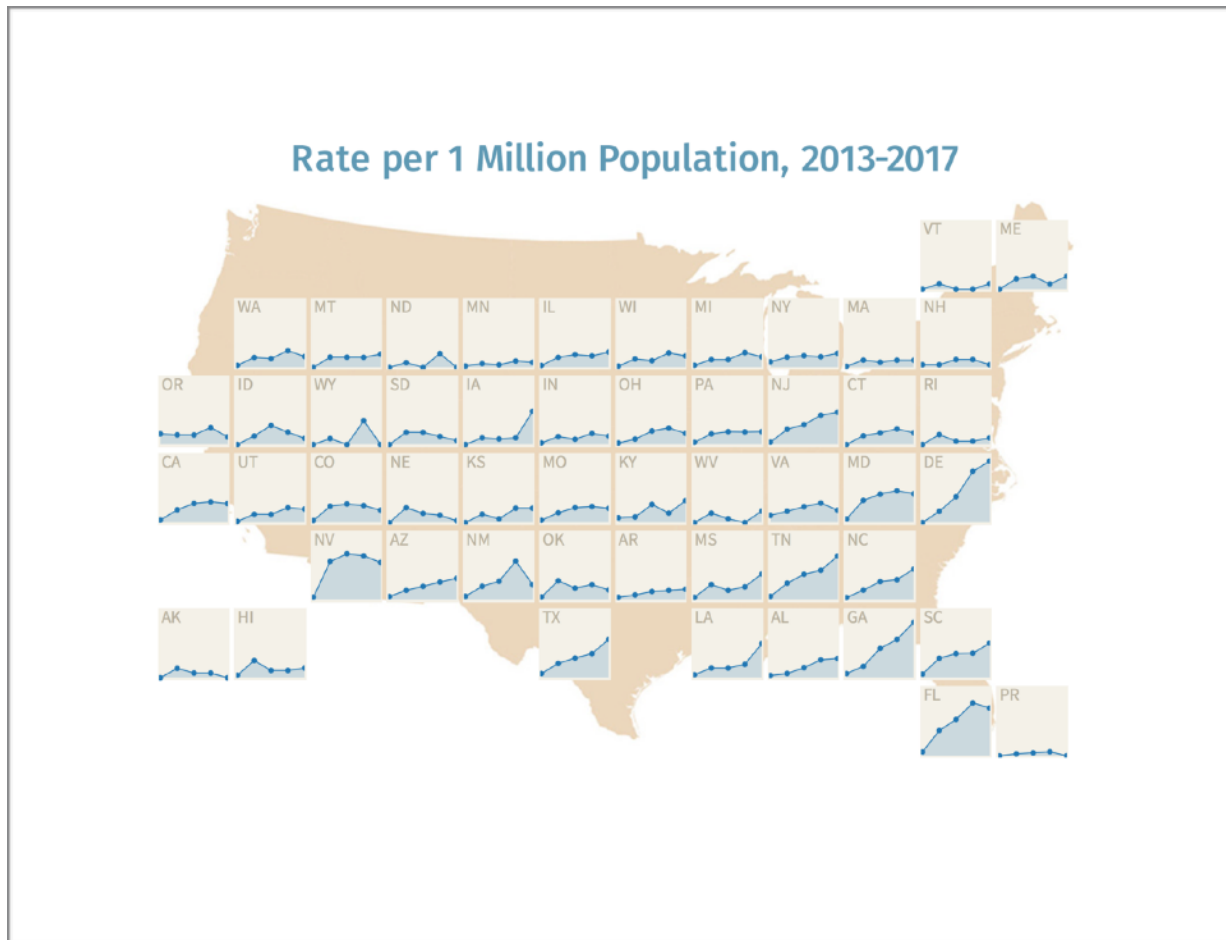
Figure 15: Rate per 1 Million Population, 2013-2017. Each dot represents one year, and the line of dots in each box represents the overall volume and change in rates of consumer medical identity theft-related complaints. Complaints adjusted for population density. Data visualization: John Emerson.

The role of medical data breaches in medical identity theft complaint activity

Medical data breach statistics are important to consider in attempting to quantify medical identity theft activity and impacts. That medical data breach statistics are being reported

to HHS and are made available to the public is a positive development. In the consumer complaint data, medical data breach does show up as an issue in consumer narratives. But it does not do so in a way that can be systematically studied or compared with the HHS medical breach data. We hypothesize that there are multiple intersecting data sets that could be found relating to medical identity theft and medical data breaches. However, those data streams, despite the richness of the medical data breach data, are not yet fully available.

It would be extremely useful for HHS to facilitate ongoing consumer feedback about the short, medium, and long term impact of medical data breaches on those affected. For example, giving breach victims the ability to report back on medical debt collection arising post-breach notification would be an important statistic to collect over the course of time. Much more needs to be done to give medical breach victims a continuing voice, and allow for their formal complaint input on long-term impacts from specific breaches. If, for example, a patient receives a notice of medical data breach, and then one or two years later receives debt collection attempts on medical debt, this would be an important statistic to capture.

Until better data integration is available, only the most general analysis is possible.

US Department of Health and Human Services, Visualization of HHS medical data breach notification data, 2009-2016

WPF has conducted regular analysis of the HHS medical data breach data, and has created a map of the data.

As discussed previously, it is simply not possible at this time to directly correlate medical data breaches to specific consumer complaint patterns of medical identity theft, except in rare instances. It is possible to notice broad trendlines.

On the World Privacy Forum website, the map below is interactive. For this report, a static image has been used. The interactive version of the map is available at: https://www.worldprivacyforum.org/2016/09/2016-breach-interactive/. On the website, the data can be sorted by year, region, listing, or a combination.
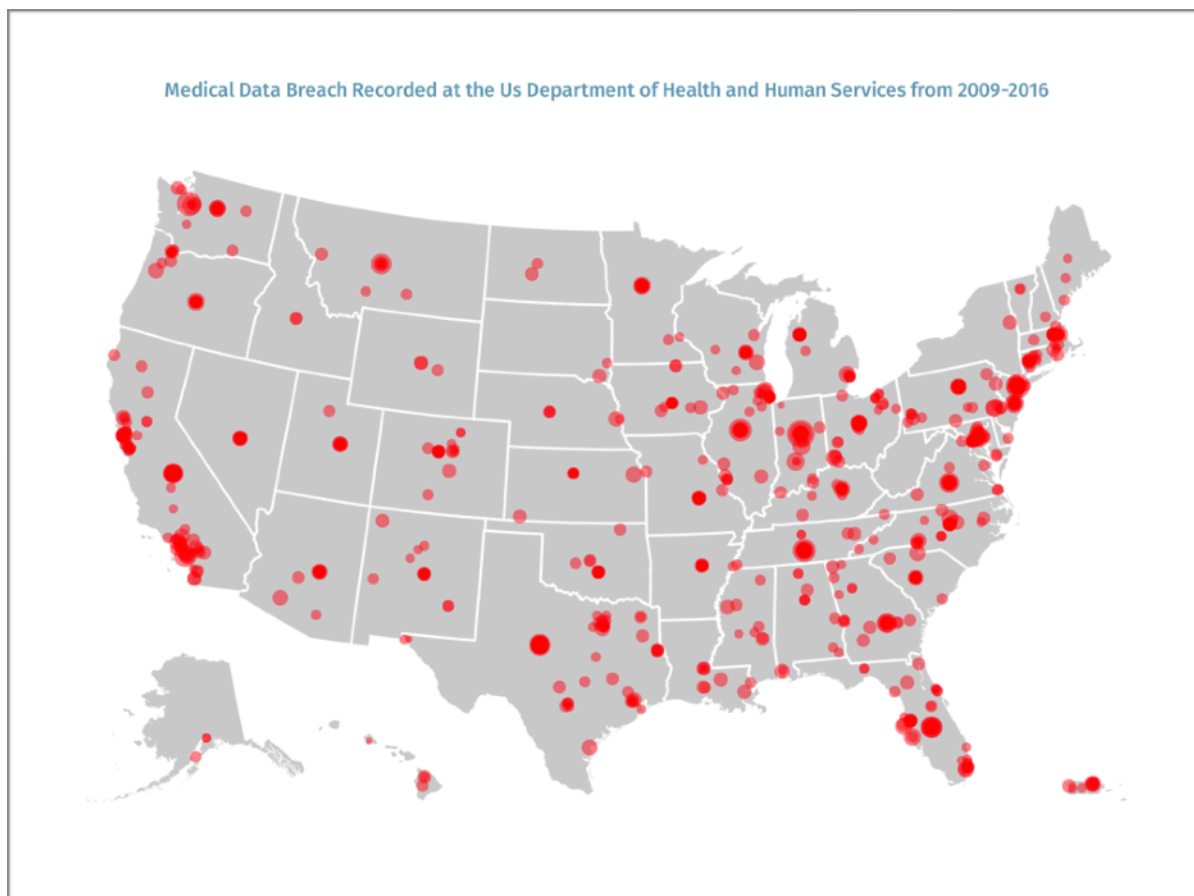
Figure 16: Visualization of HHS medical data breach occurrences from 2009-2016. Dot size represents total number of records breached. An interactive version of this map is available on the World Privacy Forum web site, https://www.worldprivacyforum.org/ 2016/09/2016-breach-interactive/. Data visualization: John Emerson.

Again, it is difficult to draw sharp geographic conclusions from the medical breach data. The Northern and Southern California breach hot spots can also be seen in the city-level map of the FTC data. What the causes of the similarity are is not possible to discern from the data at this time. The broad trend of increased activity on the Eastern seaboard edging all the way nearly to the middle of the country is also similar in some aspects to the FTC city level data. But much more work will need to be done to quantify how medical data breaches are directly impacting patients, and whether or not those patients are experiencing higher levels of impacts specifically from medical identity theft.

One of the clearest ways to ascertain this relationship could be to track debt collection attempts on medical debt resulting from identity theft from people who have been subject

to one or more data breaches. Debt collection is emerging as a long-term harm arising from medical identity theft activities. Much more work needs to be done in this area.

IV. Debt Collection Consumer Harms: Medical Debt Resulting from Identity Theft

Although WPF's analysis initially focused on geographic distribution and growth patterns of medical identity theft, the CFPB database also revealed striking new documentation and detail regarding debt collection and victims of medical identity theft, and gave new insight into the mechanisms of medical identity theft modalities and consumer impacts and harms. These data are analyzed in detail in the forthcoming Part 3 of this report series. However, the findings are significant and provide new information, thereby warranting a condensed inclusion here.

In the consumer-reported medical identity theft complaint data to the CFPB, much geographic data could be gleaned. Some data included consumer narratives. These narratives, written by the consumers, consistently described considerable life harms arising from medical debt collection related to medical forms of identity theft. It has been clear since 2006 that some medical identity theft victims first learn of the crime through a debt collection process. Yet full documentation of the many harms and activities of medical debt collection on identity theft victims has not been as available for study until now.

Debt collectors and victims of medical identity theft

The CFPB data includes consumers who have self-reported problems related to debt collection of medical debt not owed as a result of identity theft. A subset of this data is a group of complaints about medical debt not owed as a result of identity theft, and the debt collector continues to make ongoing attempts to collect on debt the consumer does not owe. When consumers provide detailed narratives about their experiences, and hundreds have done so, it is possible to determine many aspects of how medical identity theft is happening, and the impacts of medical identity theft in relation to debt collection.

The narrative data reveal that:

- Victims of medical identity theft may experience egregious and aggressive debt collection for medical services they did not seek or receive.
- Victims of medical identity theft may experience recurring debt notices in their credit bureau reports as a result of sales of medical debt. Even if a victim clears their file once, after the debt is sold, the new debt collector may report that debt as fresh. The

victim is forced to go through another cycle of removing the fraudulent information from their credit bureau files.

- Victims of medical identity theft may experience significant life harms based on the actions of debt collectors attempting to collect on debt resulting from medical identity theft. For example, continuing poor credit leading to an inability to qualify for home loans.
- Victims of medical identity theft can experience years of harassment in the aftermath of the crime. Some narratives mention 1 to 3 years of debt collections resulting from medical identity theft.

The narratives have also revealed a new variant of medical identity theft, which is fraudulent debt collection of medical bills that were not owed. The mechanism is that a debt collector begins to send fake bills and demands directly to the patient. When patients object or request verification of the debt, the debt collector typically reports debt to the credit bureau, and then demands payment to remove it, even when no payment is owed. Some of these victims were not originally victims of medical identity theft. The fraud occurred at the medical debt collection level.

The victims' perspectives: the profound harms resulting from medical identity theft debt collections

These consumer narratives add a great deal of knowledge to our understanding of how debt collections on medical identity theft victims are being handled, and the news is not good. It is not unusual whatsoever to read in the CFPB data that consumers are experiencing debt collectors reporting debt due to medical identity theft one, two, and three years after consumers first reported the problem and disputed the fraudulent bills. There is a clear problem with debt collections for victims of medical identity theft, and this problem can and should be remedied.

Healthcare providers that pass debt resulting from medical fraud onward to collections is the first part of the problem. The second aspect of the problem, in looking at the data, appears to be related to medical debt buying and selling. Some consumers experienced reappearance of their debt after it had been removed. Other consumers simply cannot get debt from medical identity theft off of their credit reports — the collectors continue to report the debt, and too frequently appear to refuse to remove it despite consumers filing police reports and other documents.

Here is a small sampling of the narratives consumers have submitted regarding their experiences. Spelling and grammar errors have been left as is and the text has been preserved as it appeared in the dataset.

Complaint ID 1793614
2/18/12
Florida

> *i am experiencing issues involving my identification which has been used in the opening of medical accounts that have been appearing on my credit reports since xxxx over the past 3 years i have asked that the (xxxx) bureaus assist me with acquiring verification from this company so that i can move forward in the removal of the entry from my credit history.*

Complaint ID 2575151
7/13/13
Florida

> *in xxxx of xxxx i noticed a debt collection listed on my xxxx credit file with syndicated office systems aka central financial control that was fraudulent in the amount of xxxx. I immediately contacted them to dispute the item. I have been disputing this debt with syndicated/central financial to no avail. I had previously provided an affidavit and police report of identity theft requesting the debt be removed due to fraud. I spoke to an representative numerous times for almost two years and nothing has happened. I continued to send the affidavit and the police report for now almost two years. I call and now they tell me that they will only respond to me via me making a fax request as it has been reported as fraud. I do n't know what else to do when i have provided the identity theft police report and affidavit of identity theft as to this xxxx debt. It has affected my ability to obtain credit for almost two years now and has caused me irreparable harm.*

Complaint ID 1400663
5/31/11

> *i was advised by the internal revenue service that my social security number and other confidential information were compromised. Sometime in xx/xx/xxxx to xx/xx/xxxx my personal details were stolen and have been used up to xxxx xxxx when a security alert had been placed on my credit files. These fraudulent accounts range from medical ; utility accounts and credit card accounts and must be deleted from my history. I forward the details of these accounts in question and a copy of the identity theft affidavit and i have had no response from xxxx the credit bureaus and the creditor/collections agent.*

Complaint ID 2080186
8/24/12

Illinois

> *i have several medical bills from this company, and i never seen these people in my life. I 've been an id theft victim for a long time, and i 'm very upset. These need to come off of my credit too!*

Complaint ID 2283050
1/10/13
Washington

> *i have disputed the credit account multiple times and the account still remain on all xxxx of my credit profiles. I have also obtained a police report stating i was a victim of identity theft. I have asked for this account to be removed numerous amounts of times but to no avail. Please help me remove this inaccurate information from my credit file as it is affect my life as well as my family. I have medical insurance through my provider of 7 years and never visited this xxxx*

Complaint ID 1829972
3/12/12
Ohio

> *commonwealth financial systems has placed an item on all xxxx of my credit bureaus that was proven to a previous collection agency as fraudulent. I have contacted this collection agency several times and they will not return telephone calls or mailings, but also refuse to remove the item from my credit reports. The item in question is from a hospital bill in xxxx xxxx that took place by a person using information from my stolen wallet. The original debt is from xxxx xxxx xxxx hospital, and i have a statement xxxx xxxx xxxx xxxx hospital detailing that their investigation resulted in my being free and clear from further collection attempts because they found the incident to be a case of identity theft.*

Complaint ID 2470946
4/25/13
Texas

> *commonwealth financial sys tem has placed xxxx negative items on my credit report. I 've reached out to the company several times. When i called with the account number they refused to speak with me unless i give them my social security number and date of birth.   Which will allow them to update the information. I refuse to provide the information.   This account was generated by xxxx hospital. A place i 've never step foot in. They have threatened me by saying they will have me served on my job. Garnish paycheck. O ne representative stated i was a liar, and i need to pay the bill.   The date open is xxxx   2016 reported as collection xxxx*

Complaint ID 1612295
10/16/11
Virginia

> *someone used my identity for medical services. I filed the proper police report and the debt collection company still refuses to remove the debt from my credit report. I also requested a copy of the bill with signature but the debt company refused.*

Complaint 1398899
5/29/11
Michigan

> *someone used my id in xx/xx/xxxx and xx/xx/xxxx. I pulled my credit report found a {$15000.00} (!!)) bill from montery collections in xxxx. I sent a debt validation letter they sent back a letter stating " the defaulted account will continue to be reported accordingly " it 's in dispute and on my credit!!! Copy letter attached.*
> *The computer printed generic contract does n't have my signature, just a printout. They did not validate the debt, nor answer all my questions asking for copy contract my signature, copy their bond and license number, copy papers showing i agree to pay, nothing. They are not licensed to collect debt in state of xxxx.*
> *They did not send a copy of the agreement showing they are authorized to collect debt on someone 's behalf, nor the name and address of the original creditor as requested.*
> *I am sending a xxxx letter, which is attached hereto., by registered mail. I am writing the attorney general of xxxx and of michigan as well as the ftc.*

Complaint 2048931
8/4/12

> *i was xxxx at xxxx hospital, xxxx xxxx, florida, on sunday, xxxx xxxx, xxxx and was discharged on wednesday, xxxx xxxx, xxxx. On friday, xxxx xxxx, xxxx, i paid my account in full in person in the amount of {$5800.00}. On xxxx xxxx, xxxx i received the official receipt from the hospital for full payment of my account.*
>
> *On thursday, xxxx xxxx, xxxx, i stopped at the emergency rooms, receptionist, specifically to obtain the address of xxxx xxxx xxxx, the xxxx who had attended to me while i was at the hospital. Xxxx xxxx xxxx kindly gave me the address and had a friendly chat with me, including her personal background. I was not*

admitted, nor was i treated, and was assured that there will be no charge for this interaction. End of narrative.

On xxxx xxxx, xxxx, i was telephoned by the hospital 's account management operation in xxxx, that there was a balance on my account of {$230.00} for the emergency room interaction on xxxx xxxx, xxxx, for which i had been assured there was no charge. On pointing this out to the person i spoke with, and upon further checking, she agreed that there was a notation on the account to that effect, that is, no additional charge. Nevertheless, on xxxx xxxx, xxxx i received a phone call from xxxx in xxxx that was intimidating in tone and content, and claiming that an additional charge of {$230.00} was now owed. I was upset and disconcerted and wrote to xxxx xxxx xxxx xxxx, chief executive officer of the hospital, with a copy to the hospital 's accounting office, on xxxx xxxx, xxxx but received no reply from either.

To my utter astonishment, between xxxx xxxx, xxxx and xxxx xxxx, xxxx, i received several letters from various collection agencies with no identification of the services provided, demanding different amounts of payment from {$1500.00} to {$230.00}, and most recently, {$450.00}. On xxxx xxxx, xxxx my husband and i replied to cmre financial, disputing their claim of {$1.00} and also attaching a copy of our letter to xxxx xxxx xxxx xxxx. We received no response. In between, i received a letter of apology from the xxxx xxxx xxxx xxxx xxxx, dated xxxx xxxx, xxxx, stating " we apologize for this error and the inconvenience this incident (notice from a collection agency indicating balance due) has caused ".

As a last resort, we contacted the hospital twice, on xxxx xxxx, xxxx and xxxx xxxx, xxxx using the " contact us " feature on their website, detailing our aggravating story and have been harassed relentlessly by debt collection agencies, and requesting that the balance on my account be corrected and reflect the accurate amount which is xxxx. Both messages were computer-acknowledged but no response whatsoever was forthcoming.

This very stressful and protracted situation has been going on for more than three years with neither the hospital nor the various debt collectors taking any responsibility to respond and to fully correct the record.

We would be most grateful for your assistance in correcting this matter.

The impact of debt collection on victims of medical forms of identity theft is a significant harm that needs to be addressed by all stakeholders in meaningful and effective ways.

V. Conclusion and Recommendations

Medical identity theft is alive and well in the United States. The crime is growing, and the consumer complaint data analyzed for this report suggests that the crime is not distributed equally across the United States; some states have a bigger problem with the crime than others. The data visualizations in this report show that geographic hot spots can shift and change over time. However, the data suggests that the southeastern US region is experiencing more incidents of medical identity theft than other regions, judging by consumer complaints. Some other states outside of the southeastern region also reveal patterns of increased activity.

In the consumer complaint data, new documentation of the actions of medical debt collections of victims of medical identity theft revealed new aspects of harms to victims, including long term harms ranging from 1 to 3 years.

It is possible, from the data, to take several incremental steps forward in the understanding of medical identity theft.

- We can now securely hypothesize that the crime of medical identity theft will typically have uneven distribution across the US, and that this distribution will reflect not just population size, but more likely focused activity of criminals in certain regions.

- We can now suggest with some degree of confidence that the southeastern United States has emerged as a zone of increased consumer complaints about medical identity theft. This uptick could generally indicate increased medical identity theft activity in the region.

- We can now securely state that debt collection is an integral aspect of the harms many medical identity theft victims experience. It is more integral than has been previously documented. It is possible that debt collection is the primary way that victims learn they are victims of the crime.

- We are not ready to directly correlate medical data breaches to patterns of medical identity theft. There are very loose correlations, and the narrative data from consumers did contain information from data breach victims. But much more systemic data is needed to make assured judgements.

Recommendations:

- The geographical patterns of medical identity theft that have been suggested by the consumer complaint data need to be further quantified. Additional studies conducted by US government agencies are needed to determine what the specific incidence of medical identity theft is nationally, how and where it is occurring, and how it can be detected and prevented.

- The existence of medical identity theft hotspots suggested by the data should be considered by members of law enforcement, health care officials, community leaders, members of civil society, and others working directly with consumers in areas that may be in zones of potential increased activity.

- Notification of medical data breaches to consumers has the potential to save lives, protect health, and prevent losses. The notification process is now in place at HHS. Now, it is important to ensure that victims of medical data breaches can report their experiences of breach impacts in a systematic way. Post-breach debt collection and other tangible, detectible, provable harms could be reported to HHS so as to more fully document consumer impacts. WPF recommends that HHS facilitate patients' ability to document at the HHS breach portal debt collection of medical debt they do not owe after they have received a breach notice. This kind of collection would go far in increasing understanding of the long term impacts of the crime.

- Healthcare providers, insurors, and other stakeholders need to craft specific guidelines and procedures as to how to handle medical debt in light of what is happening to victims of medical identity theft. Medical debt collection from medical identity theft is frequently outsourced or handed off from a healthcare provider to a debt collection agency. Patients who are victims of breaches and medical identity theft need an assured way to solve problems arising from debt collectors who refuse to validate their debt, remove debt notices from credit bureau files, and other onerous behavior. This is a significant cause of harm and much more needs to be done to address this harm.

- All healthcare providers need comprehensive risk assessments focused on preventing medical identity theft while protecting patient privacy. These risk assessments need to include specific plans for handling patient impacts, including file errors, debt collection practices, and other impacts. After healthcare providers have passed debt to a collection agency, there needs to be a mechanism of retracting that debt from the debt collection process.

- The CFPB should monitor medical debt collection activities resulting from medical identity theft and address debt collectors that show up as repeat offenders in consumer narratives and complaints.

Report Credits:

Research, analysis, writing: Pam Dixon

Data visualization, analysis: John Emerson

For More Information:

For updates to this report and other documents related to the report, see the World Privacy Forum's Medical Identity Theft page at <http://www.worldprivacyforum.org/ medicalidentitytheft.html>

Contact:

World Privacy Forum

www.worldprivacyforum.org

info@worldprivacyforum.org

 +1 760.436.2489

The World Privacy Forum is a 501 (C) (3) non-profit, tax-exempt organization. Its focus is on public interest research and consumer education relating to privacy topics.