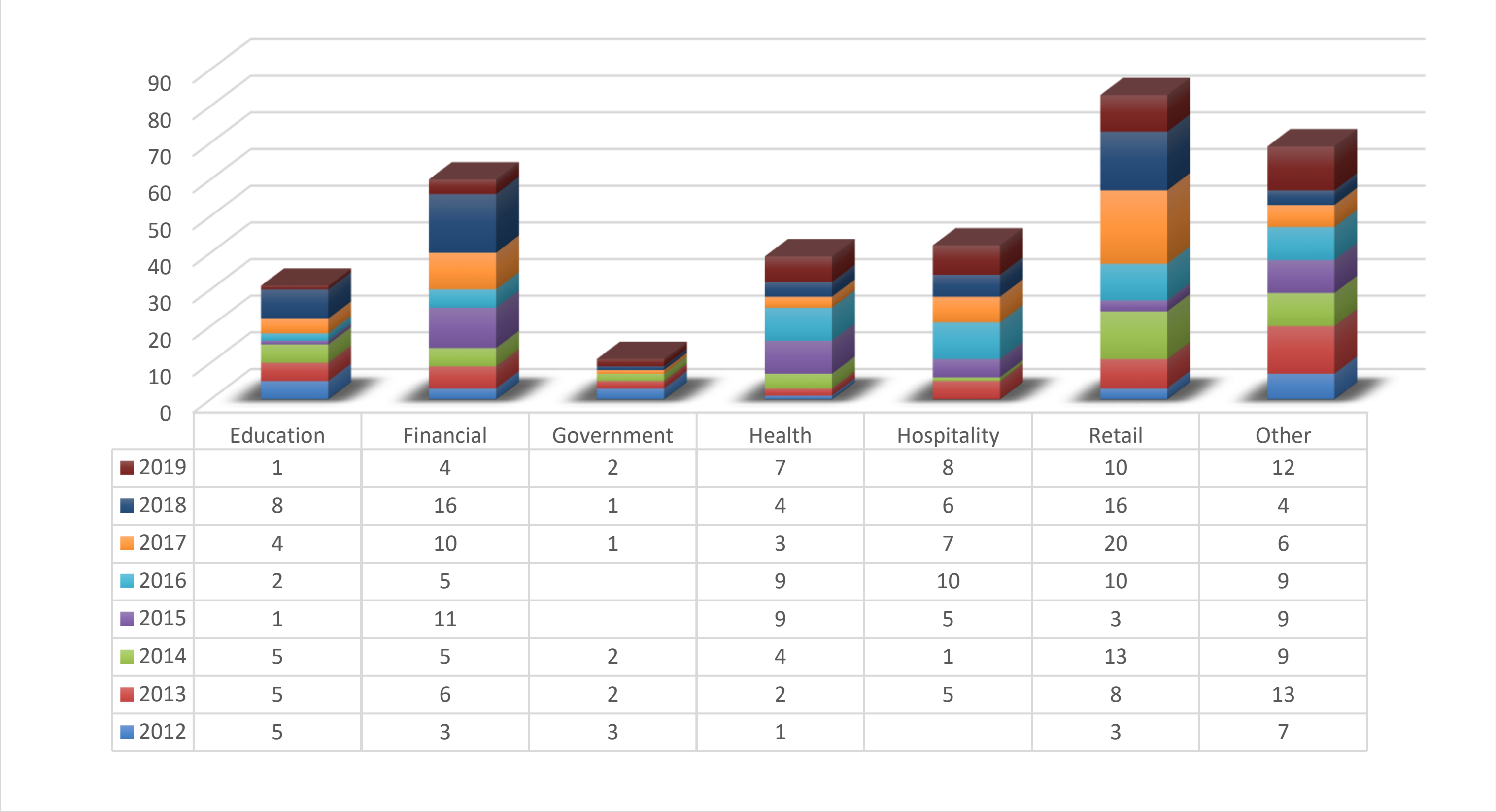
South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

Security Breach Notice Report

An overview of the security breach notices received by SCDCA since 2012 as well as a detailed analysis of the security breach notices received in 2019.

2020

Number of Security Breach Notices Received by Industry
January 2012 – December 2019



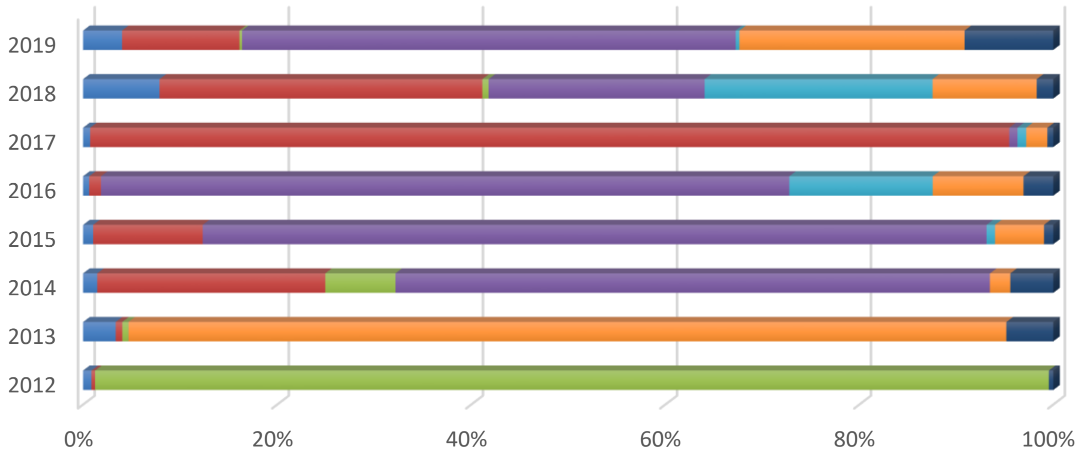
	Education	Financial	Government	Health	Hospitality	Retail	Other
2019	1	4	2	7	8	10	12
2018	8	16	1	4	6	16	4
2017	4	10	1	3	7	20	6
2016	2	5		9	10	10	9
2015	1	11		9	5	3	9
2014	5	5	2	4	1	13	9
2013	5	6	2	2	5	8	13
2012	5	3	3	1		3	7

Figure 1

From January 2012 through December 2019, SCDCA received **335** breach notices. A total of thirty-one were reported by education providers, sixty from financial service providers, eleven from governmental entities, thirty-nine from healthcare organizations, forty-two from the hospitality industry, and eighty-three breaches from the retail industry. SCDCA also received sixty-nine reports of breaches from organizations outside these six main categories.

SCDCA received the most notices in 2018 (55 notices) followed closely by 2017 (51 notices). The notices received in years 2013 through 2019 represent a significant increase in comparison to 2012 (22). However, the number of notices received decreased in 2019 (44) compared to 2018 (55).

Number of South Carolina Residents Affected by Security Breaches by Industry
January 2012 – December 2019



	2012	2013	2014	2015	2016	2017	2018	2019
🟦 Education	35,611	18,210	937	6,457	1,781	19,328	38,646	33,458
🟥 Financial	15,177	3,686	15,179	70,736	3,485	2,521,407	163,351	100,956
🟩 Government	4,045,416	3,341	4,666			105	3,200	2,216
🟪 Health		59	39,577	505,998	202,745	22,606	109,311	424,391
🟦 Hospitality		12		5,495	42,274	23,991	115,451	3,283
🟧 Retail	75	491,156	1,356	31,651	26,768	58,220	52,771	193,713
⬛ Other	19,001	26,246	2,861	5,963	8,770	16,013	8,376	76,347

Figure 2

Over 9.6 million[1] South Carolina residents were affected by the 335 security breaches reported during 2012–2019. Cumulatively, 2012 represented the year with the largest number of South Carolina residents being affected by breaches with 4,115,280, despite there being only 22 notices that year. The total number of residents affected by breaches for the remaining years addressed in this report are as follows: 834,364 (2019); 491,106 (2018); 2,661,670 (2017); 285,823 (2016); 626,300 (2015); 64,576 (2014); and 542,710 (2013).

Although the number of affected consumers varied significantly among the different industries and organizations, the government sector breaches in 2012 impacted the largest number of South Carolina consumers at 4,045,416. Reported breaches involving financial organizations affected the most consumers in 2017 (2,521,407) and 2018 (163,351). Healthcare organizations reported breaches affecting the most consumers for the years 2014 (39,577), 2015 (505,998), 2016 (202,745) and 2019 (424,391). Breaches reported by the retail industry affected the most consumers in 2013 (491,156 consumers).

[1] Please be aware as you read the information provided that many companies and organizations were unable to report a specific number of consumers affected, even after a thorough investigation had been completed. In these instances, the number of consumers affected was recorded as "0." Therefore, the totals provided reflect the minimum number of South Carolina residents potentially affected and the actual number is likely significantly higher.

Total Number of Notices and Affected Consumers per Industry
January 2012 – December 2019

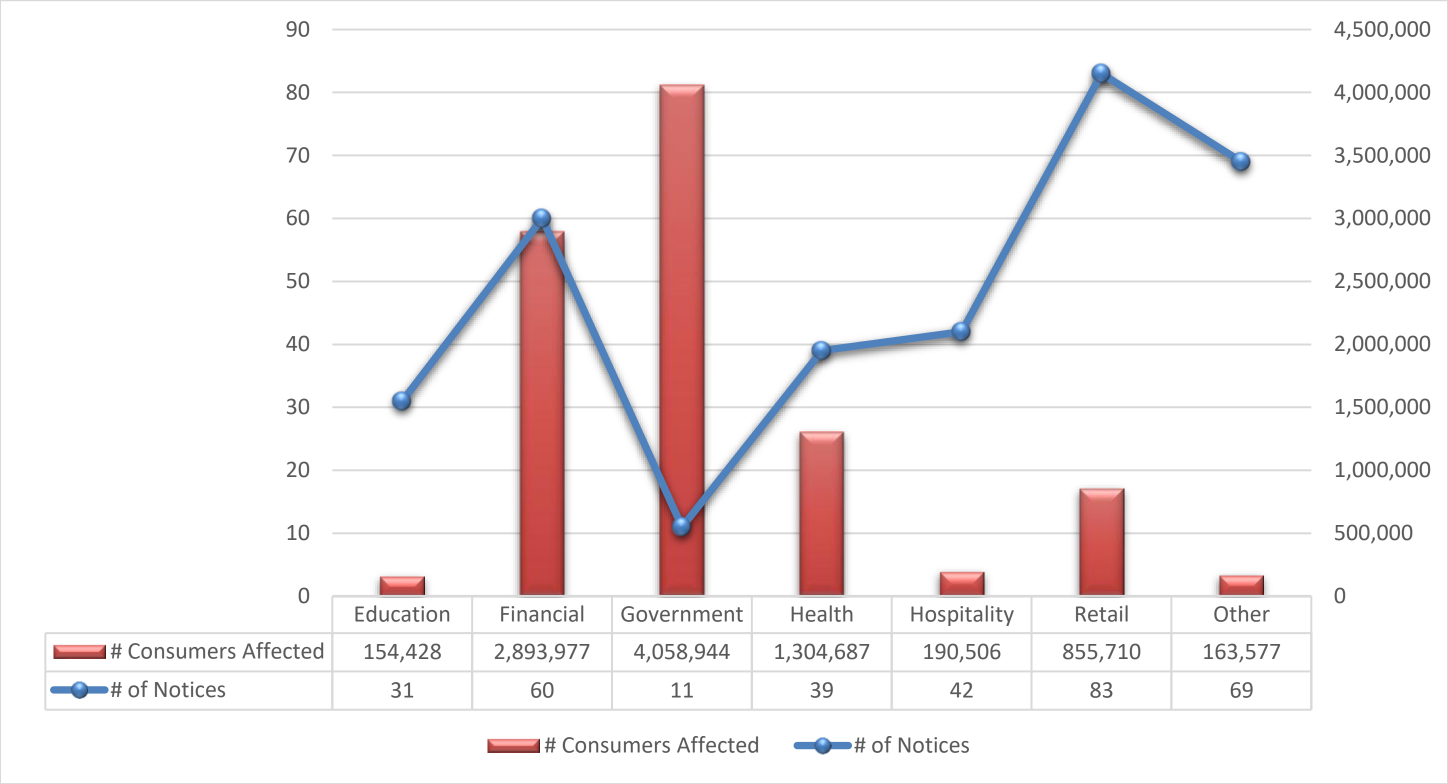
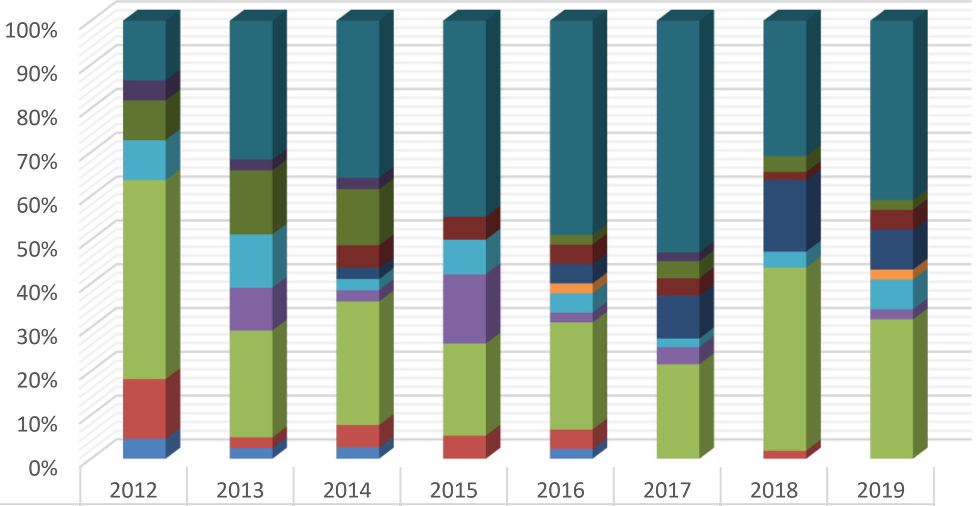


Figure 3

From January 2012 through December 2019, Education providers reported thirty-one security breaches affecting 154,428 residents. Financial service providers reported sixty security breaches affecting nearly 2.9 million residents. Governmental entities reported eleven security breaches affecting more than four million South Carolina residents. The healthcare industry reported thirty-nine security breaches that affected over 1.3 million residents. The hospitality industry reported forty-two breaches, which affected 190,506 residents. The retail industry reported eighty-three security breaches that affected 855,710 residents. Other industries falling outside these six main sectors filed sixty-nine notices affecting 163,577 consumers.

Types of Breaches
January 2012 – December 2019



	2012	2013	2014	2015	2016	2017	2018	2019
■ Hacking - malicious attacks on computer networks	13.64%	31.71%	35.90%	44.74%	48.89%	52.94%	30.91%	40.91%
■ Improper disposal of documents - personal data left in documents deposited in publicly accessible garbage bin	4.55%	2.44%	2.56%	0.00%	0.00%	1.96%	0.00%	0.00%
■ Loss of IT equipment - misplaced or stolen equipment - laptops, USB sticks, etc.	9.09%	14.63%	12.82%	0.00%	2.22%	3.92%	3.64%	2.27%
■ Mailing - distribution of a letter in the mail or an email to an incorrect address that includes personal data	0.00%	0.00%	5.13%	5.26%	4.44%	3.92%	1.82%	4.55%
■ Phishing Attack	0.00%	0.00%	2.56%	0.00%	4.44%	9.80%	16.36%	9.09%
■ Ransomware Attack	0.00%	0.00%	0.00%	0.00%	2.22%	0.00%	0.00%	2.27%
■ Technical error - unforseen complication in an IT system exposing data to outside parties	9.09%	12.20%	2.56%	7.89%	4.44%	1.96%	3.64%	6.82%
■ Theft - data in the form of documents, electronically stored data, etc. that is stolen	0.00%	9.76%	2.56%	15.79%	2.22%	3.92%	0.00%	2.27%
■ Unauthorized access - employee or outside party improperly attained access to system	45.45%	24.39%	28.21%	21.05%	24.44%	21.57%	41.82%	31.82%
■ Unauthorized disclosure - e.g. distributing personal data on peer-to-peer networks	13.64%	2.44%	5.13%	5.26%	4.44%	0.00%	1.82%	0.00%
■ Other	4.55%	2.44%	2.56%	0.00%	2.22%	0.00%	0.00%	0.00%

Figure 4

From 2012 to 2019, the most prevalent types of breaches have been hacking (131) and unauthorized access (98). SCDCA has received four breach reports due to the improper disposal of documents; nineteen due to a loss of IT equipment; eleven due to mailing errors; twenty-one due to phishing attacks; nineteen caused by an unforeseen technical error; fifteen due to theft; eleven caused by unauthorized disclosure; and four caused by other circumstances.

In Depth Look at the Types of Breaches in 2019

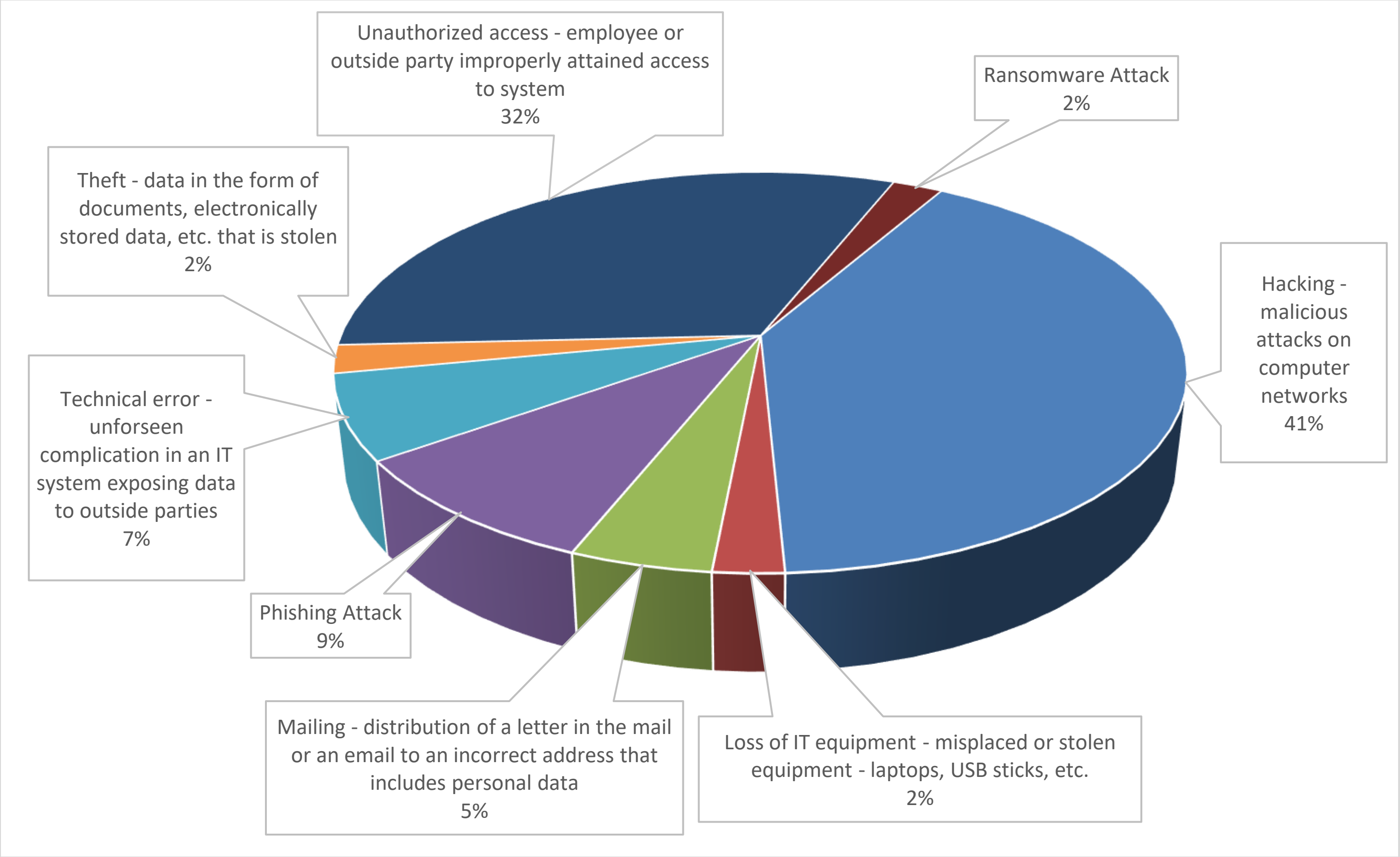
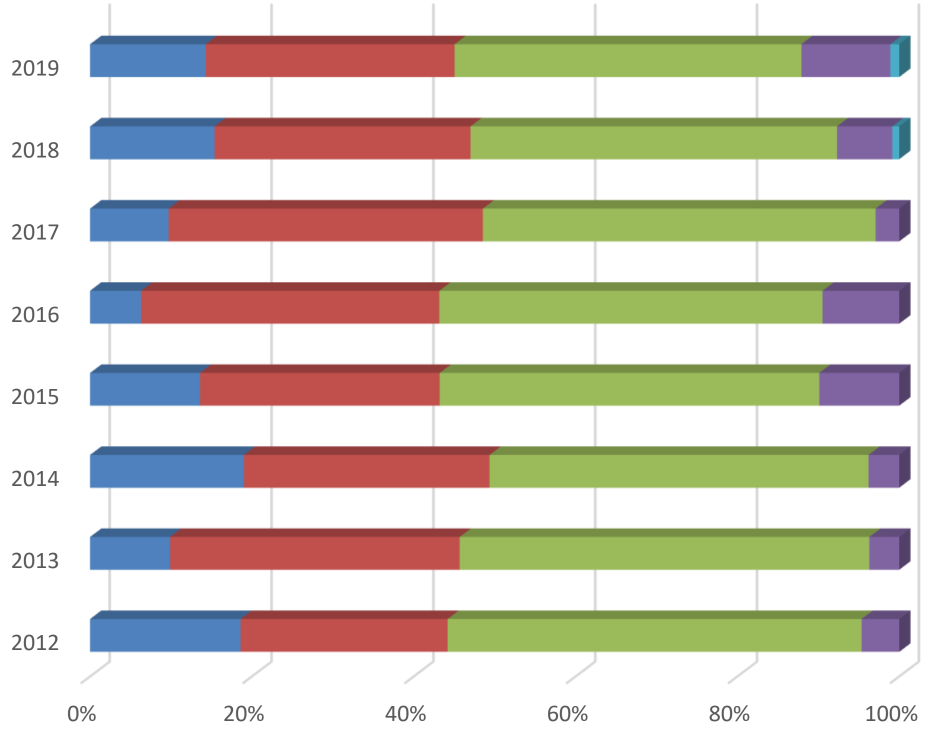


Figure 5

In 2019, SCDCA received eighteen reports of security breaches due to hacking. Three reports were due to technical errors. One report was due to theft. Fourteen security breach reports were to due general unauthorized access to PII. One security breach reported was due to a loss of IT equipment. Two security breach reports were caused by mailing errors. Four security breach reports were due to phishing attacks.

Notably, there were no security breach reports received in 2019 due to the improper disposal of documents or unauthorized disclosure. This could indicate that organizations are paying more attention to how PII is handled and disposed. Furthermore, hacking and phishing attacks seem to have played bigger roles in 2019 (causing forty-one percent and nine percent of reports) compared to the historical rate of thirty-seven percent and five percent, respectively.

Types of Data Breached
January 2012 – December 2019



	2012	2013	2014	2015	2016	2017	2018	2019
🟦 Credential Data (personal email, account username/password)	8	8	15	11	6	10	18	13
🟥 Financial Data (credit/debit card numbers, income, financial transactions, bank statements, etc.)	11	29	24	24	35	40	37	28
🟩 Personal Data (SSN/Tax ID, full name, address, driver's license no.)	22	41	37	38	45	50	53	39
🟪 Protected Health Data (diagnoses, treatment info, test results, etc.)	2	3	3	8	9	3	8	10
🟦 Other							1	1

Figure 6

From 2012 to 2019, SCDCA has received eighty-nine security breach reports implicating credential data; two-hundred and twenty-eight indicating a breach of financial data; three-hundred and twenty-five implicating personal data; forty-six indicating compromised protected health data, and two indicating a breach of other types of potentially sensitive information, including location data and academic history.[2]

[2] SCDCA's methodology recognizes that multiple types of data can be breached within one security breach.

In Depth Look at the
Types of Data Breached in 2019

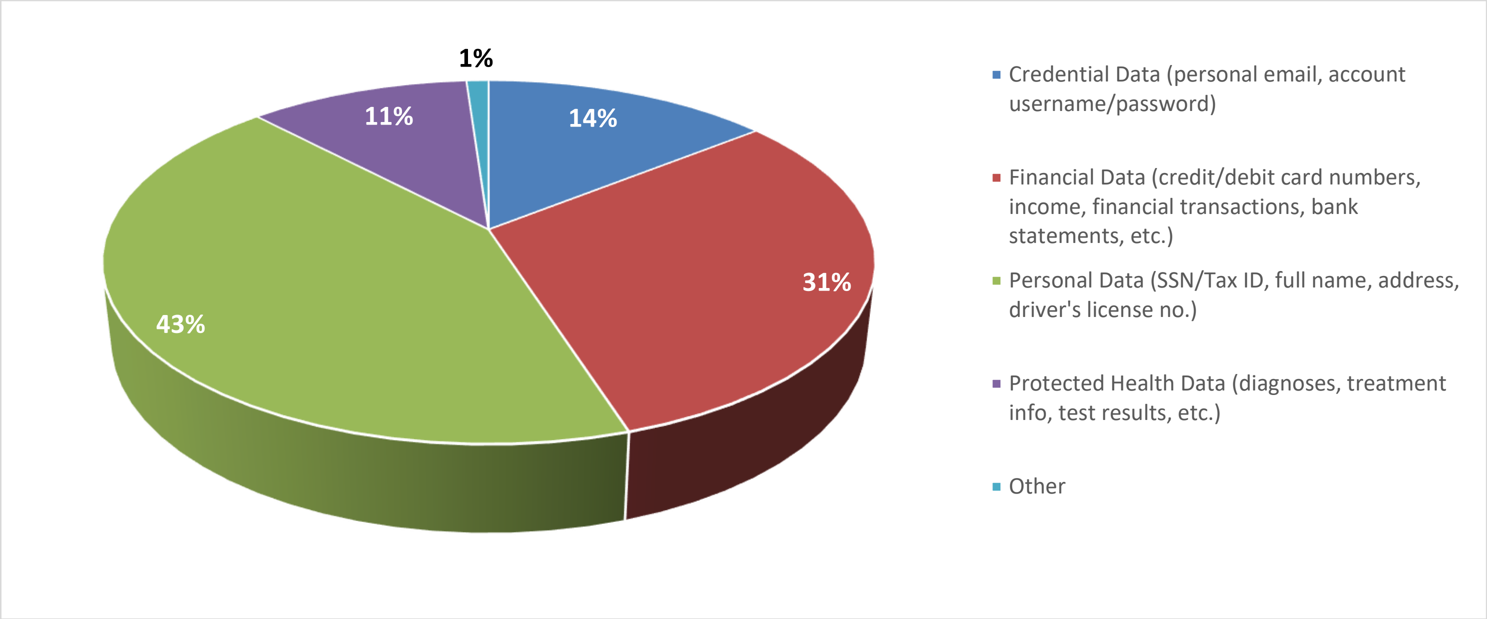


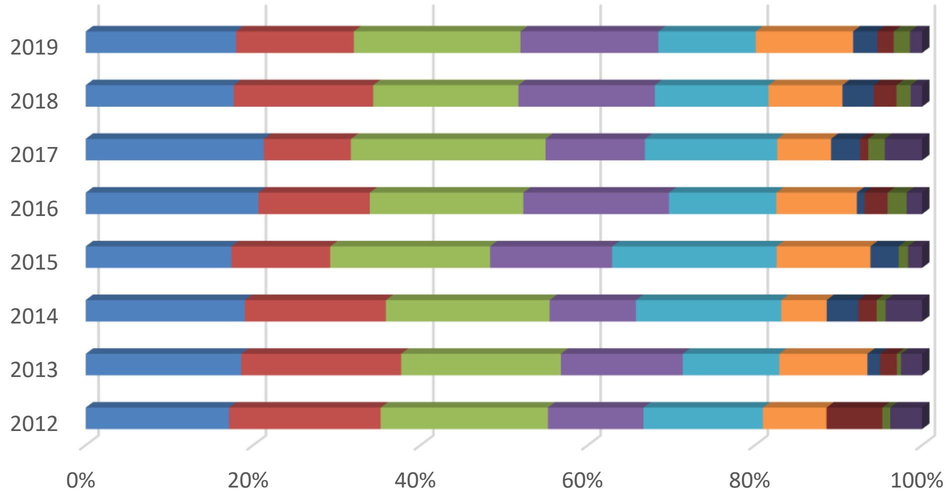
Figure 7

In 2019, SCDCA received thirty-nine notices of breached personal data; twenty-eight notices of compromised financial data; thirteen notices related to credential data; ten reports of breached protected health information; and one report which included potentially exposed location data.

Notable trends in the type of data breached in 2019 includes the increase of exposed protected health data. Historically, the yearly average[3] percentage of breaches involving protected health data is 12%. However, in 2019, nearly 23% of reported breaches involved the exposure of protected health data. Conversely, the breach of personal data decreased by roughly 10%; financial data decreased by 1%; and credential data increased by 4%.

[3] Average of all breaches reported to SCDCA from January 1, 2012, through December 31, 2019.

Remediation Steps Taken by Reporting Organizations
January 2012 – December 2019



	2012	2013	2014	2015	2016	2017	2018	2019
■ Full assessment of security measures	18	37	35	31	45	43	52	37
■ Established call center for consumers	19	38	31	21	29	21	49	29
■ Provide consumer education on identity theft and fraud	21	38	36	34	40	47	51	41
■ Fix data vulnerability issue(s)	12	29	19	26	38	24	48	34
■ Credit monitoring services offered to affected consumers	15	23	32	35	28	32	40	24
■ Implement additional security safeguards	8	21	10	20	21	13	26	24
■ Require users to change passwords		3	7	6	2	7	11	6
■ Implement Policies & Procedures	7	4	4		6	2	8	4
■ Change business network passwords	1	1	2	2	5	4	5	4
■ Other	4	5	8	3	4	9	4	3

Figure 8

In 2019, SCDCA began capturing the remediation steps taken by the reporting organizations and completed a review of the steps taken in previously-reported beaches, as well.[4] From 2012–2019, 298 organizations initiated a full assessment of their security measures; 237 established a dedicated call center for affected consumers; 308 provided consumer education on identity theft and fraud; 230 fixed data vulnerability issues; 229 offered free credit monitoring services to affected consumers; 143 implemented additional security safeguards; 42 required users to change their passwords; 35 implemented policies and procedures related to protecting sensitive data; 24 changed their business network passwords; and 40 took remediation steps outside of the other nine categories. Some examples of other remediation measures taken include: the implementation of two-factor authentication, employee training, termination of third-party contracts, and the addition of encryption software.

[4] SCDCA's methodology tracks multiple remediation steps taken by an organization in response to a security breach.

In Depth Look at the Remediation Steps Taken by Reporting Organizations in 2019

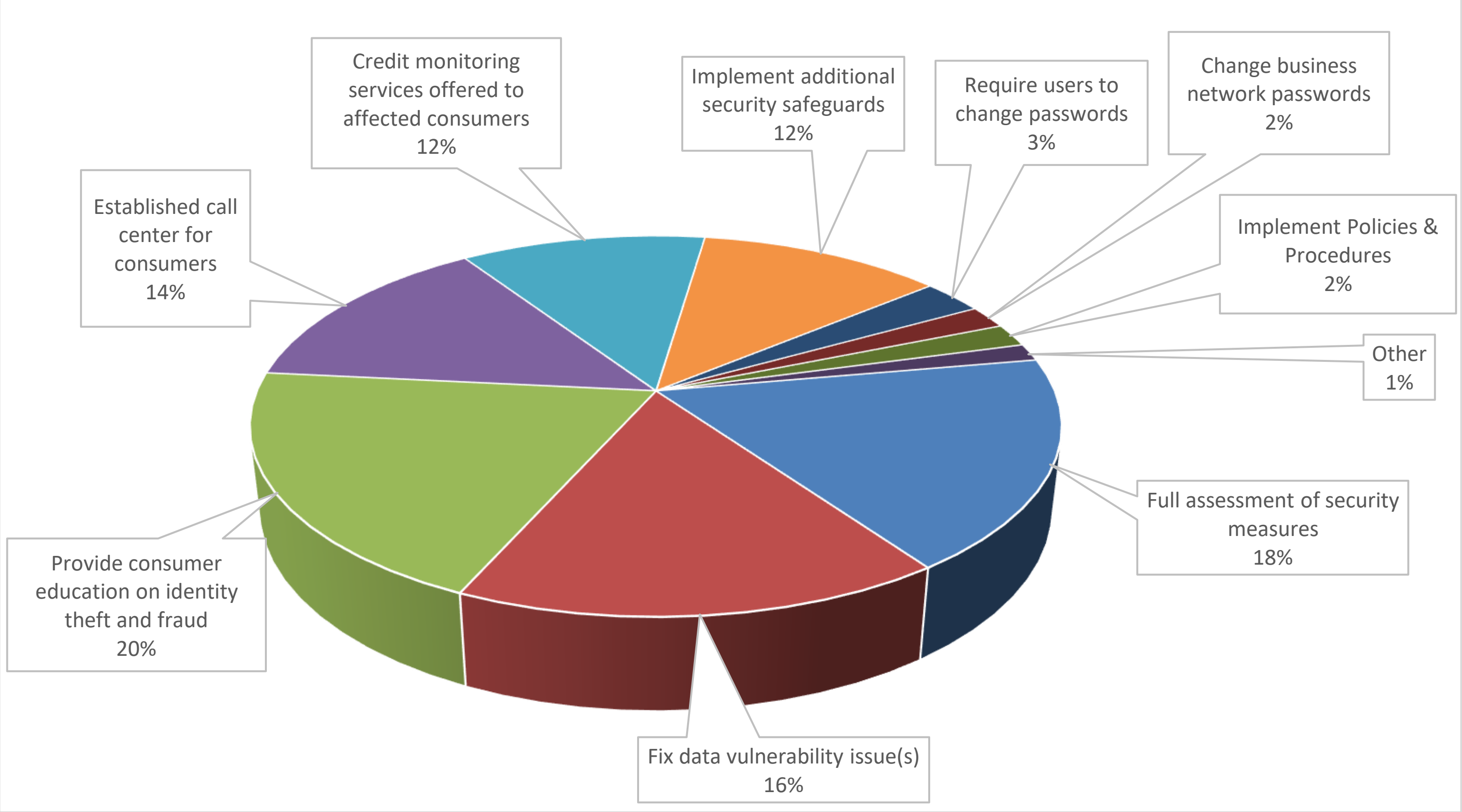


Figure 9

In 2019, thirty-seven organizations undertook a full assessment of their security measures; thirty-four fixed data vulnerability issue(s); forty-one provided consumer education on identity theft and fraud; twenty-nine established call centers for affected consumers; twenty-four offered free credit monitoring to affected consumers; twenty-four implemented additional security safeguards; six required users to change passwords; four changed their business network passwords; four implemented policies and procedures; and three undertook other remediation measures, including: temporarily shutting down the breached website until all issues were resolved, implementing two-factor authentication for employees, and training employees on how to prevent future breaches.

Most of the remediation steps tracked by SCDCA have remained consistent as compared to the average of the previous seven years. However, the largest changes include a 14% increase in organizations implementing additional security safeguards and a 16% decrease in organizations offering free credit monitoring to affected consumers.

For those consumers who may have been affected by a security breach or would like more information about protecting their personal information, visit consumer.sc.gov and click the "Identity Theft Unit" button or call us toll-free at 1-800-922-1594.

For details on what action to take in resolving specific identity theft problems, consumers can contact SCDCA's Identity Theft Unit at the number above or fill out an Identity Theft Intake Form online.

South Carolina
DEPARTMENT OF CONSUMER AFFAIRS