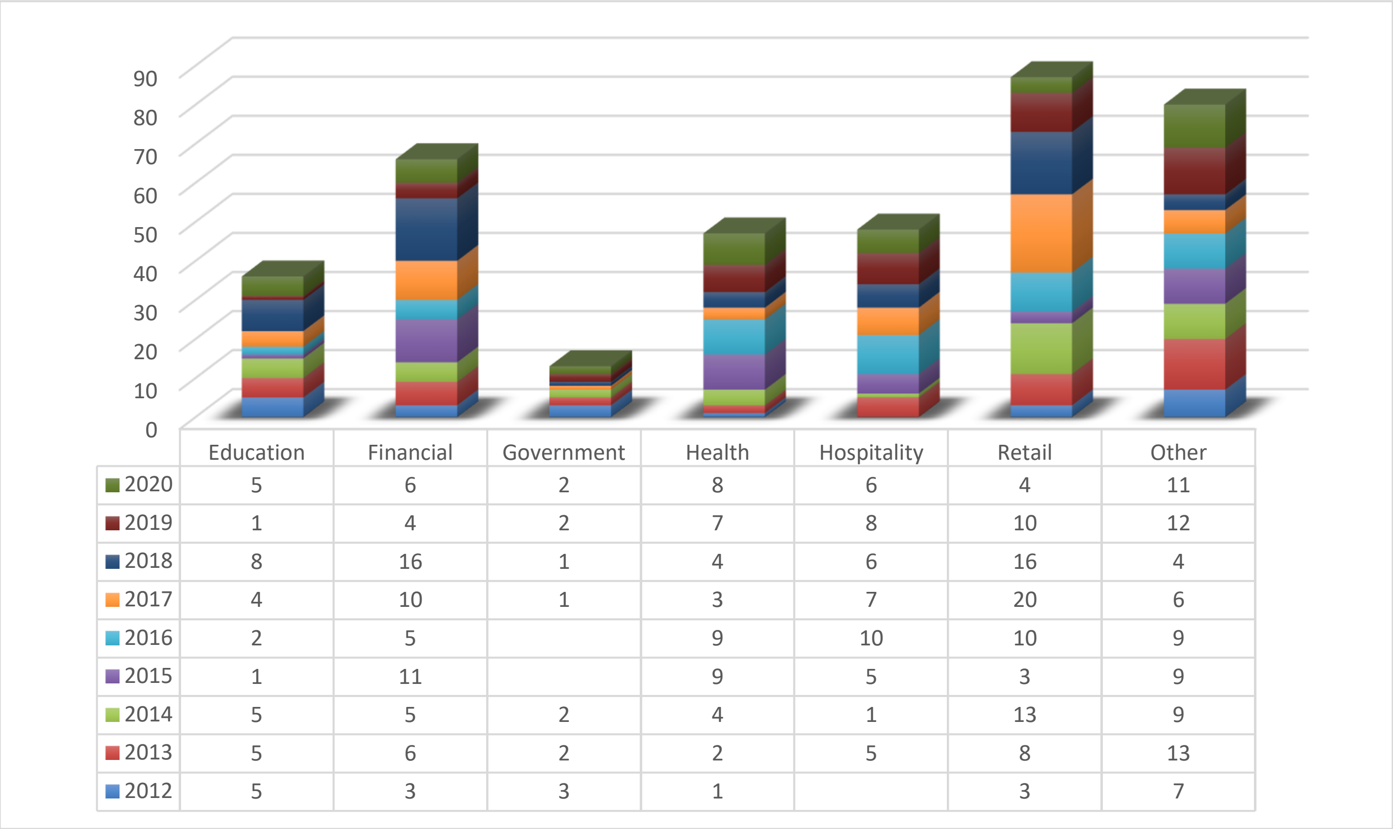
South Carolina
DEPARTMENT OF CONSUMER AFFAIRS

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 2020.

2021

Number of Security Breach Notices Received by Industry
January 2012 – December 2020



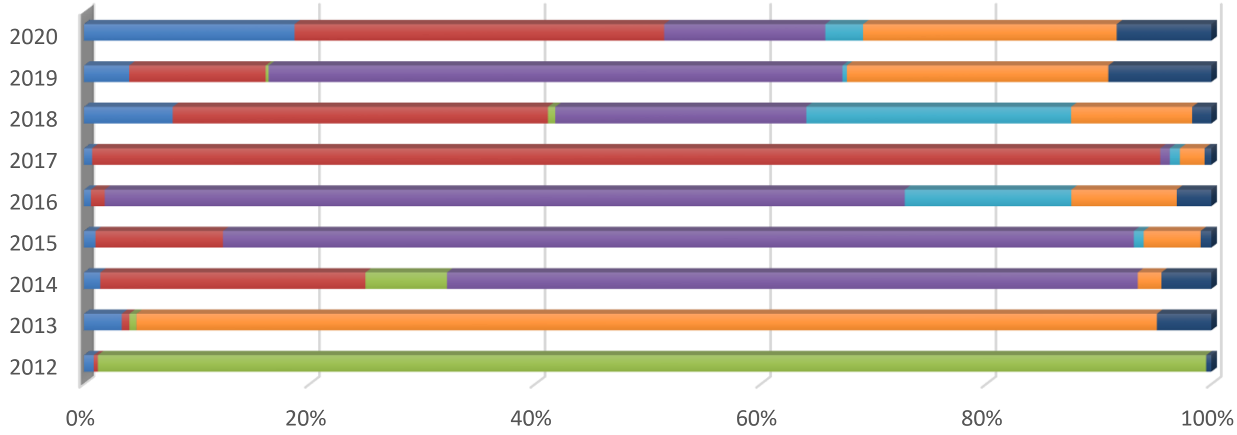
	Education	Financial	Government	Health	Hospitality	Retail	Other
■ 2020	5	6	2	8	6	4	11
■ 2019	1	4	2	7	8	10	12
■ 2018	8	16	1	4	6	16	4
■ 2017	4	10	1	3	7	20	6
■ 2016	2	5		9	10	10	9
■ 2015	1	11		9	5	3	9
■ 2014	5	5	2	4	1	13	9
■ 2013	5	6	2	2	5	8	13
■ 2012	5	3	3	1		3	7

Figure 1

From January 2012 through December 2020, SCDCA received **377** breach notices. A total of eighty-seven breaches were reported by the retail industry, sixty-six from financial service providers, forty-seven from healthcare organizations, thirty-six from education providers, forty-eight from the hospitality industry, and thirteen from governmental entities. SCDCA also received eighty 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 2020 represent a significant increase in comparison to 2012 (22). However, the number of notices received decreased in 2020 (42) compared to 2019 (44).

Number of South Carolina Residents Affected by Security Breaches by Industry
January 2012 – December 2020



	2012	2013	2014	2015	2016	2017	2018	2019	2020
🟦 Education	35,611	18,210	937	6,457	1,781	19,328	38,646	33,458	95,461
🟥 Financial	15,177	3,686	15,179	70,736	3,485	2,521,407	163,351	100,956	167,483
🟩 Government	4,045,416	3,341	4,666			105	3,200	2,216	3
🟪 Health		59	39,577	505,998	202,745	22,606	109,311	424,391	73,019
🟦 Hospitality		12		5,495	42,274	23,991	115,451	3,283	17,137
🟧 Retail	75	491,156	1,356	31,651	26,768	58,220	52,771	193,713	115,134
⬛ Other	19,001	26,246	2,861	5,963	8,770	16,013	8,376	76,347	42,951

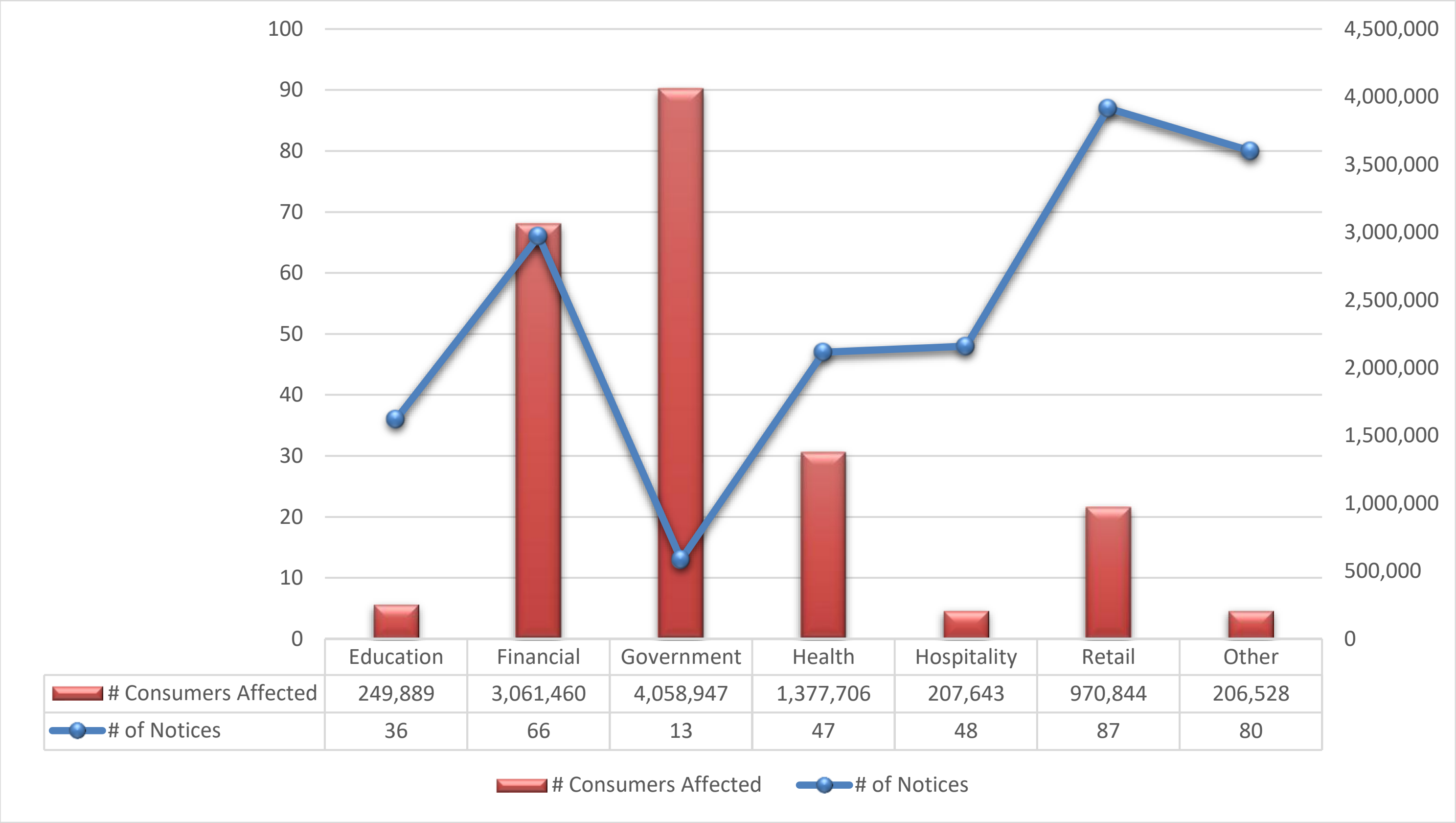
Figure 2

Over 10 million[1] South Carolina residents were affected by the 377 security breaches reported during 2012-2020. Cumulatively, 2012 represented the year with the largest number of South Carolina residents being affected by breaches with 4,115,280 – despite there only 22 notices for the year. The total number of residents affected by breaches for the remaining years addressed in this report are as follows: 511,188 (2020); 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 2020 (167,483). 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 2020

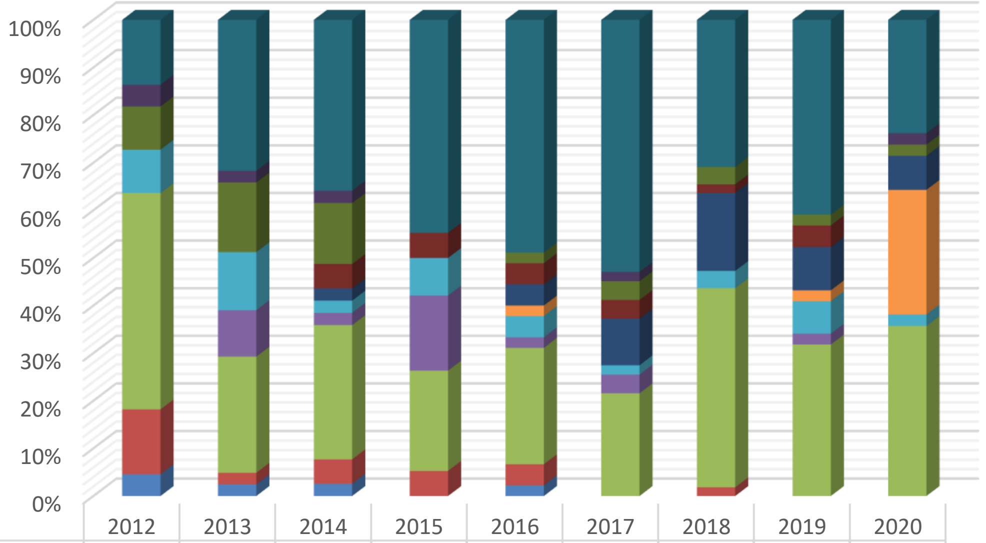


	Education	Financial	Government	Health	Hospitality	Retail	Other
# Consumers Affected	249,889	3,061,460	4,058,947	1,377,706	207,643	970,844	206,528
# of Notices	36	66	13	47	48	87	80

Figure 3

From January 2012 through December 2020, Education providers reported thirty-six security breaches affecting 249,889 residents. Financial service providers reported sixty-six security breaches affecting over 3 million residents. Governmental entities reported thirteen security breaches affecting just over four million South Carolina residents. The healthcare industry reported forty-seven security breaches that affected just under 1.4 million residents. The hospitality industry reported forty-eight breaches, which affected 207,643 residents. The retail industry reported eighty-seven security breaches that affected just under 1 million residents. Other industries falling outside these six main sectors filed eighty notices affecting 206,528 consumers.

Types of Breaches
January 2012 – December 2020



	2012	2013	2014	2015	2016	2017	2018	2019	2020
■ Hacking - malicious attacks on computer networks	3	13	14	17	22	27	17	18	10
■ Improper disposal of documents - personal data left in documents deposited in publicly accessible garbage bin	1	1	1			1			1
■ Loss of IT equipment - misplaced or stolen equipment - laptops, USB sticks, etc.	2	6	5		1	2	2	1	1
■ Mailing - distribution of a letter in the mail or an email to an incorrect address that includes personal data			2	2	2	2	1	2	
■ Phishing Attack			1		2	5	9	4	3
■ Ransomware Attack					1			1	11
■ Technical error - unforseen complication in an IT system exposing data to outside parties	2	5	1	3	2	1	2	3	1
■ Theft - data in the form of documents, electronically stored data, etc. that is stolen		4	1	6	1	2		1	
■ Unauthorized access - employee or outside party improperly attained access to system	10	10	11	8	11	11	23	14	15
■ Unauthorized disclosure - e.g. distributing personal data on peer-to-peer networks	3	1	2	2	2		1		
■ Other	1	1	1		1				

Figure 4

From 2012 to 2020, the most prevalent types of breaches have been hacking (141) and unauthorized access (113). SCDCA has received five breach reports due to the improper disposal of documents; twenty due to a loss of IT equipment; eleven due to mailing errors; twenty-four due to phishing attacks; thirteen due to ransomware attacks; twenty 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 2020

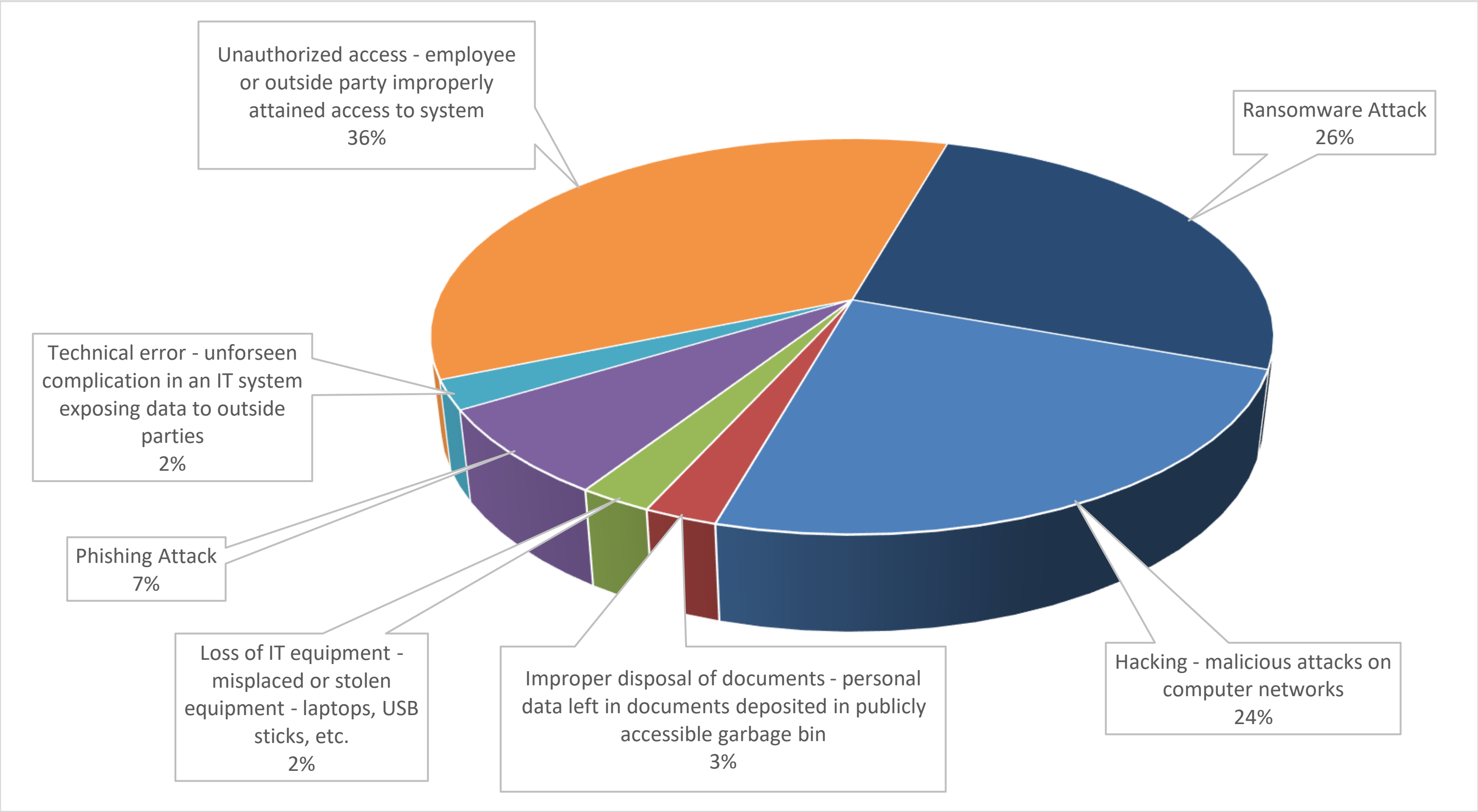
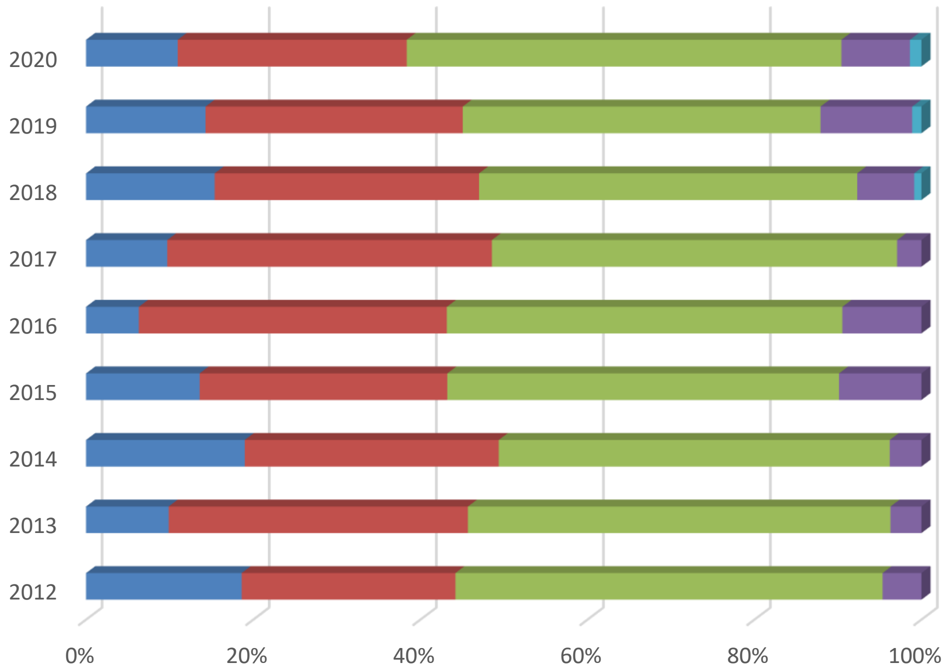


Figure 5

In 2020, SCDCA received fifteen security breach notices due general unauthorized access to PII. One breach was due to a technical error. Three security breaches were due to phishing attacks. One security breach reported was due to a loss of IT equipment. One security breach report was caused by an improper disposal of documents. Ten reports of security breaches were due to hacking. Eleven breaches were due to ransomware attacks.

Most notably, the number of ransomware attacks significantly increased in 2020 (11) as compared to previous years (2 total). In addition, there were no security breach reports received in 2020 due to mailing errors, theft, or unauthorized disclosures. Furthermore, unauthorized access has seemed to play a bigger role than hacking in 2020 (thirty-six percent and twenty-eight percent) compared to the historical rate of thirty percent and thirty-seven percent, respectively.

Types of Data Breached
January 2012 – December 2020



	2012	2013	2014	2015	2016	2017	2018	2019	2020
🟦 Credential Data (personal email, account username/password)	8	8	15	11	6	10	18	13	8
🟥 Financial Data (credit/debit card numbers, income, financial transactions, bank statements, etc.)	11	29	24	24	35	40	37	28	20
🟩 Personal Data (SSN/Tax ID, full name, address, driver's license no.)	22	41	37	38	45	50	53	39	38
🟪 Protected Health Data (diagnoses, treatment info, test results, etc.)	2	3	3	8	9	3	8	10	6
🟦 Other							1	1	1

Figure 6

From 2012 to 2020, SCDCA has received ninety-seven security breach reports implicating credential data; two-hundred and forty-eight indicating a breach of financial data; three-hundred and sixty-three implicating personal data; fifty-two indicating compromised protected health data, and three 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 2020

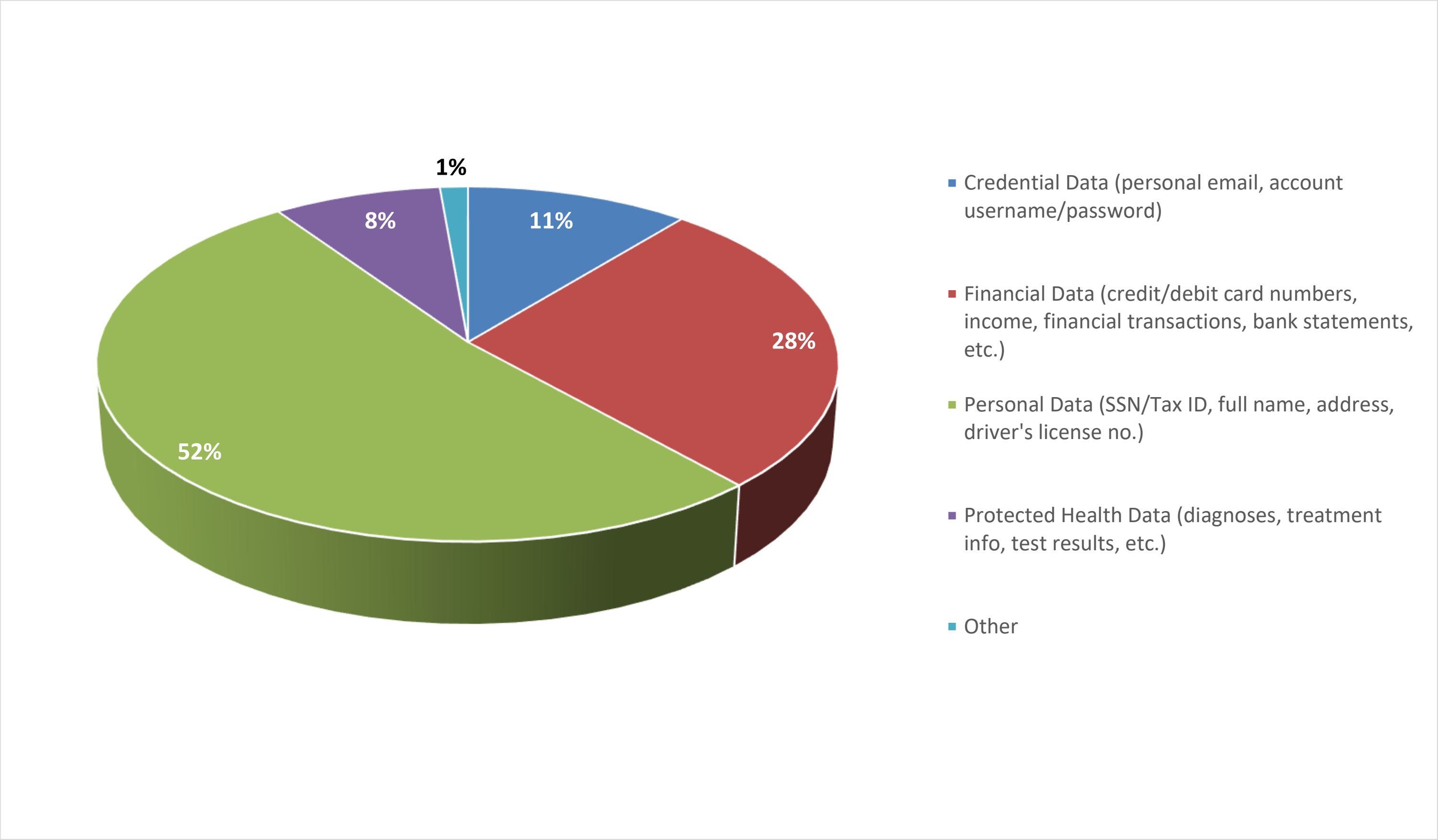


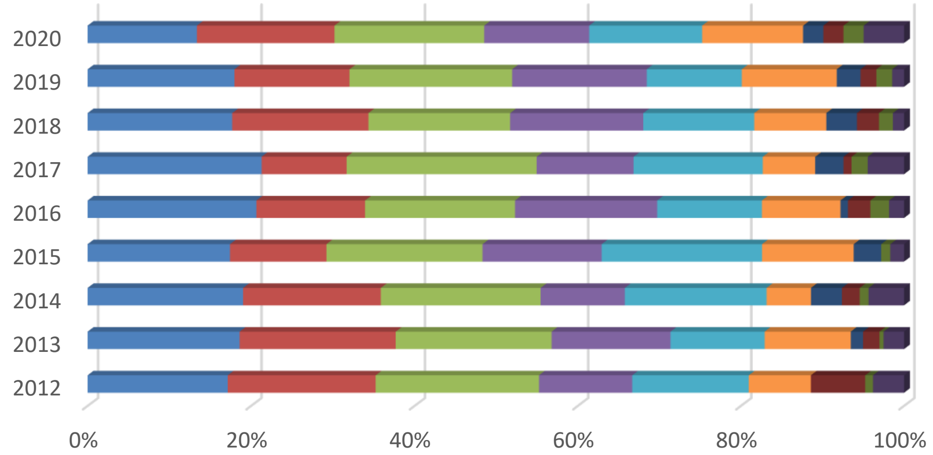
Figure 7

In 2020, SCDCA received thirty-eight notices of breached personal data; twenty notices of compromised financial data; eight notices related to credential data; six reports of breached protected health information; and one report which included potentially exposed location data.

Historically, the yearly average[3] percent of breaches involving protected personal data is 96.5%. In fact, in 2012, 2013, 2015, and 2016, 100% of the breaches reported involved the exposure of protected personal data. However, in 2020, only 90% of reported breaches involved the exposure of protected personal data. In 2020, the breach of health data increased one percentage point over the yearly average of previous years, while financial data exposure decreased by nineteen percentage points, and credential data decreased by eight percentage points.

[3] Average of all breaches reported to SCDCA from January 1, 2012, through December 31, 2020.

Remediation Steps Taken by Reporting Organizations
January 2012 – December 2020



	2012	2013	2014	2015	2016	2017	2018	2019	2020
🟦 Full assessment of security measures	18	37	35	31	45	43	52	37	27
🟥 Established call center for consumers	19	38	31	21	29	21	49	29	34
🟩 Provide consumer education on identity theft and fraud	21	38	36	34	40	47	51	41	37
🟪 Fix data vulnerability issue(s)	12	29	19	26	38	24	48	34	26
🟦 Credit monitoring services offered to affected consumers	15	23	32	35	28	32	40	24	28
🟧 Implement additional security safeguards	8	21	10	20	21	13	26	24	25
🟦 Require users to change passwords		3	7	6	2	7	11	6	5
🟥 Implement Policies & Procedures	7	4	4		6	2	8	4	5
🟩 Change business network passwords	1	1	2	2	5	4	5	4	5
🟪 Other	4	5	8	3	4	9	4	3	10

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 2012–2020, 325 organizations initiated a full assessment of their security measures; 271 established a dedicated call center for affected consumers; 345 provided consumer education on identity theft and fraud; 256 fixed data vulnerability issues; 257 offered free credit monitoring services to affected consumers; 168 implemented additional security safeguards; 47 required users to change their passwords; 40 implemented policies and procedures related to protecting sensitive data; 29 changed their business network passwords; and 50 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 2020

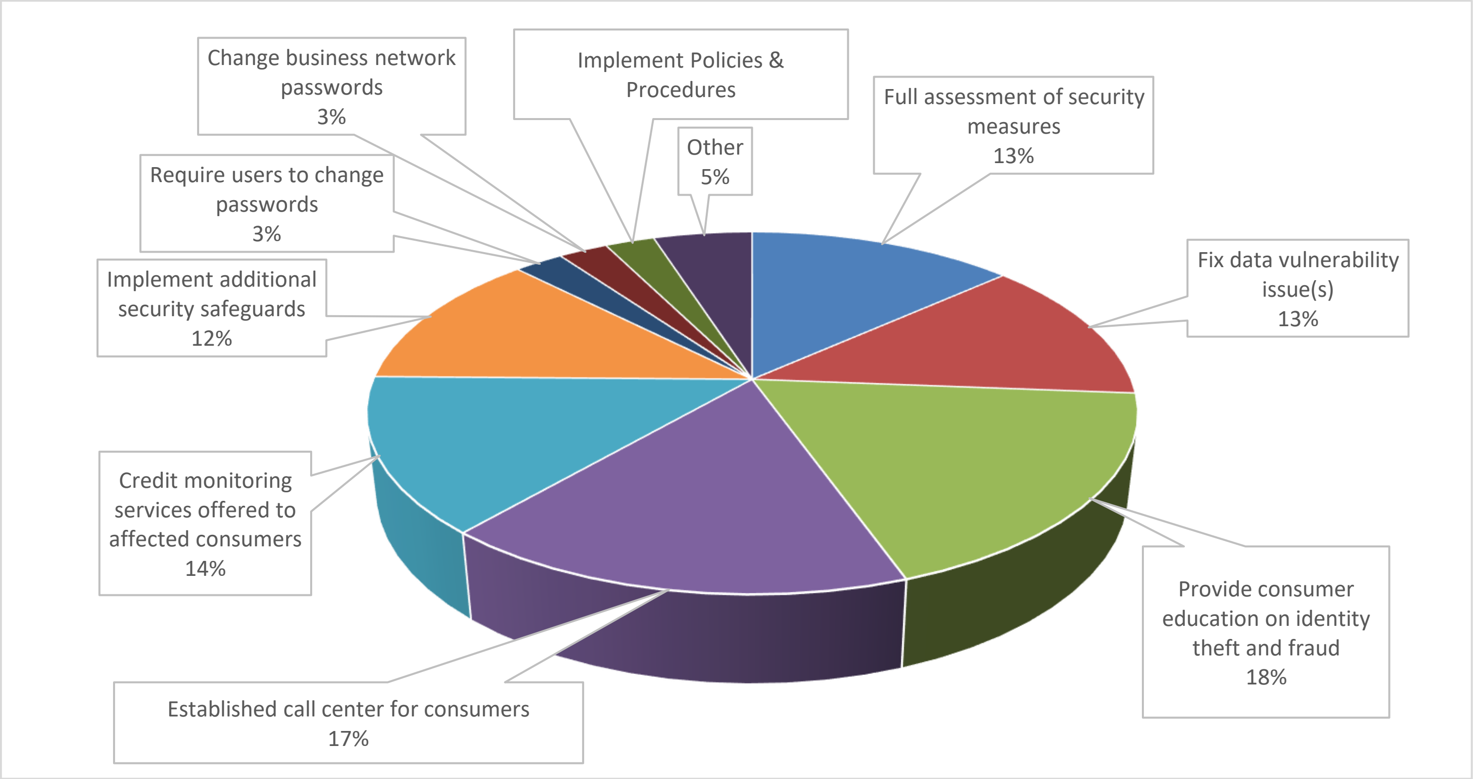


Figure 9

In 2020, twenty-seven organizations undertook a full assessment of their security measures; twenty-six fixed data vulnerability issue(s); thirty-seven provided consumer education on identity theft and fraud; thirty-four established call centers for affected consumers; twenty-eight offered free credit monitoring to affected consumers; twenty-five implemented additional security safeguards; five required users to change passwords; five changed their business network passwords; five implemented policies and procedures; and ten undertook other remediation measures, including: implementing two-factor authentication for employees, training employees on how to prevent future breaches, and deleting old consumer files to reduce the number of impacted individuals if another breach were to occur.

One of the most significant changes in 2020 from the previous 8-year average include a 24% decrease in organizations conducting a full assessment of their security measures. The substantial decline is likely due to the fact that ten reported breaches were the result of a data security incident involving a third-party vendor of a company. In such an instance, companies may not be inclined to assess their own security measures, since it was the vendor’s measures that were breached. Another significant difference in the 2020 data compared to the averages of previous years is the 11% increase in remediation measures falling in the “Other” category. The increase indicates that companies may be striving to keep up with the ever-evolving technological landscape of data security.

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