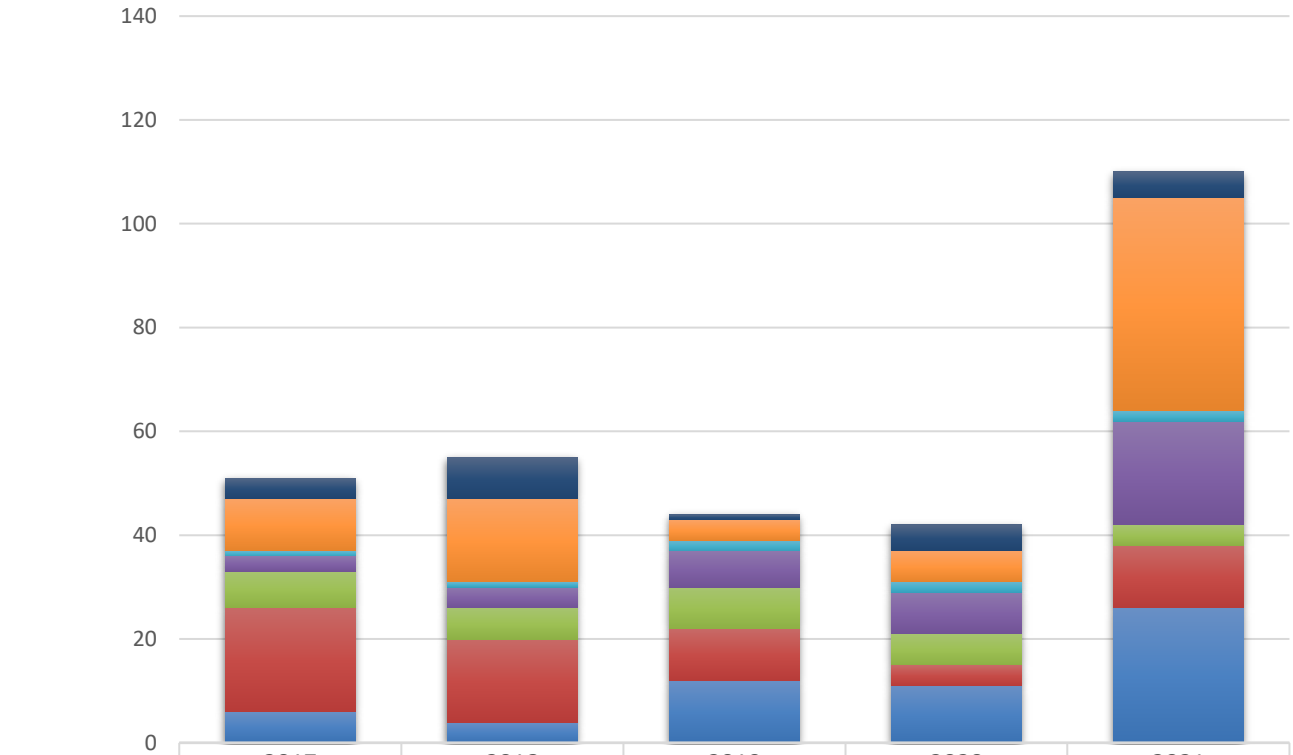
Security Breach Notice Report

An overview of the security breach notices received by SCDCA since 2017 as well as a detailed analysis of the security breach notices received in 2021.

2022

Number of Security Breach Notices Received by Industry
January 2017 – December 2021



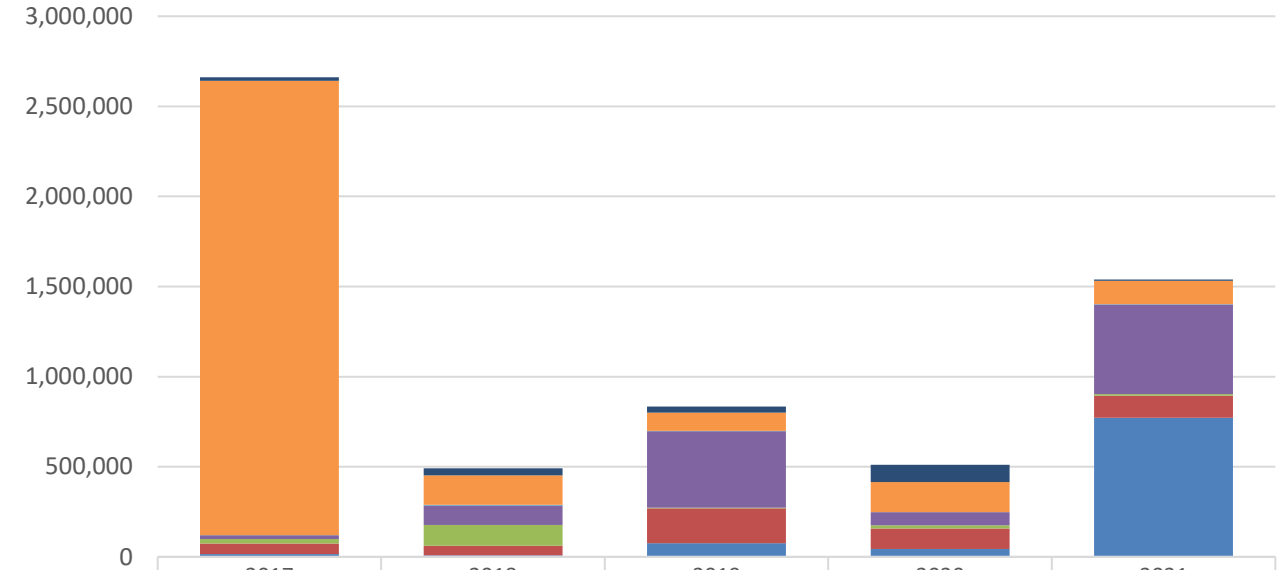
	2017	2018	2019	2020	2021
Education	4	8	1	5	5
Financial	10	16	4	6	41
Government	1	1	2	2	2
Health	3	4	7	8	20
Hospitality	7	6	8	6	4
Retail	20	16	10	4	12
Other	6	4	12	11	26

Figure 1

From January 2017 through December 2021, SCDCA received **302** breach notices. A total of seventy-seven (77) breaches were reported by financial service providers, sixty-two (62) from the retail industry, forty-two (42) from healthcare organizations, thirty-one (31) from the hospitality industry, twenty-three (23) from education providers, and eight (8) from governmental entities. SCDCA also received fifty-nine (59) reports of breaches from organizations outside these six main categories.

SCDCA received the most notices in 2021 (110 notices), doubling the number received in 2018 (55 notices), which had been the highest number reported since at least 2012. However, the number of notices received were similar in 2017 (51), 2019 (44), and 2020 (42).

Number of South Carolina Residents Affected by Security Breaches by Industry
January 2017 – December 2021



	2017	2018	2019	2020	2021
Education	19,328	38,646	33,458	95,461	8,244
Financial	2,521,407	163,351	100,956	167,483	128,910
Government	105	3,200	2,216	3	2,241
Health	22,606	109,311	424,391	73,019	498,000
Hospitality	23,991	115,451	3,283	17,137	7,811
Retail	58,220	52,771	193,713	115,134	122,248
Other	16,013	8,376	76,347	42,951	772,450

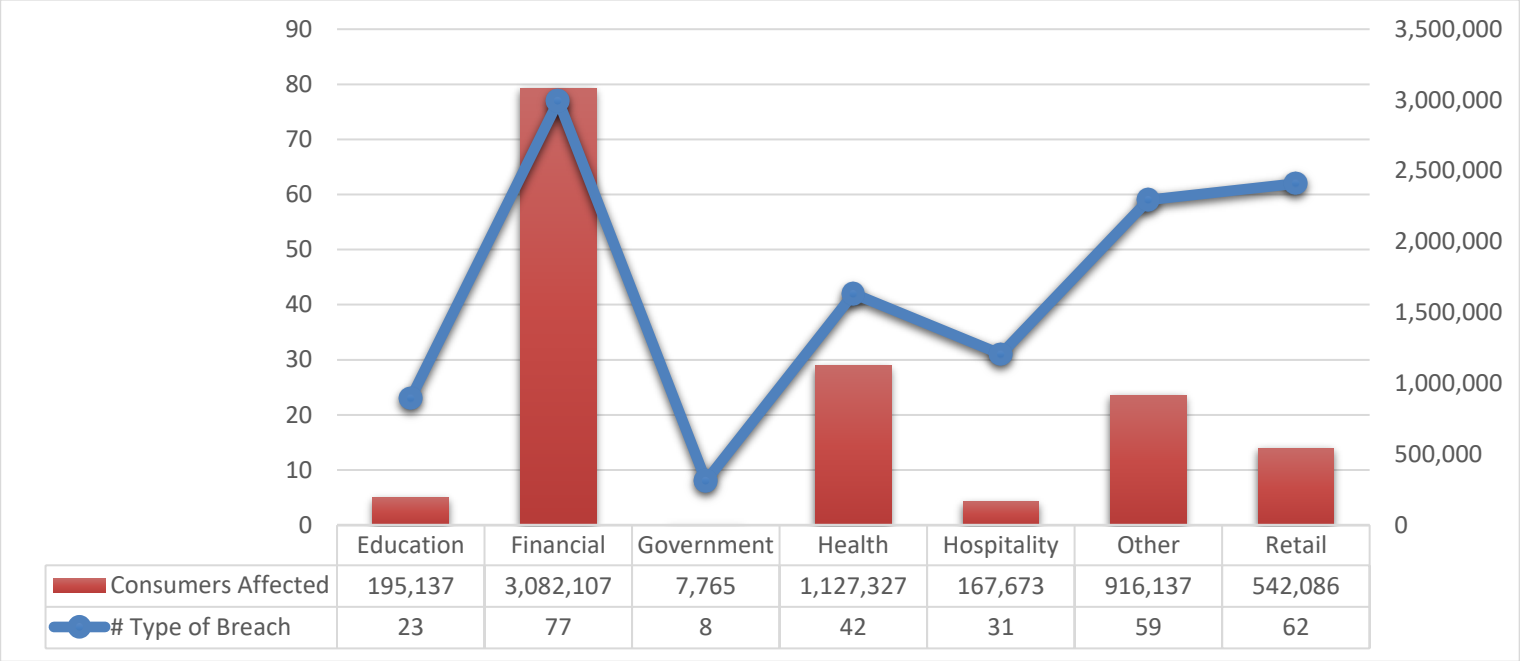
Figure 2

Over 6 million[1] South Carolina residents were affected by the 302 security breaches reported January 2017 through December 2021. Cumulatively, 2017 represented the year with the largest number of South Carolina residents being affected by breaches with 2,661,670, despite there only being 51 notices for the year. The total number of residents affected by breaches for the remaining years included in this report are as follows: 1,539,904 (2021); 511,188 (2020); 834,364 (2019); 491,106 (2018).

For breaches reported during 2017–2021, the financial sector breaches in 2017 impacted the largest number of South Carolina residents at 2,521,407. Reported breaches with organizations outside these six main categories affected the most residents in 2021 (772,450) along with healthcare organizations (498,000). Breaches reported by the financial industry affected the most residents in 2020 (167,483) and 2018 (163,351). Healthcare organizations reported breaches affecting the most residents for the years 2019 (424,391).

[1] Please be aware as you read the information provided that many companies and organizations were unable to report a specific number of residents affected, even after a thorough investigation had been completed. In these instances, the number of residents 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 Residents per Industry
January 2017 – December 2021

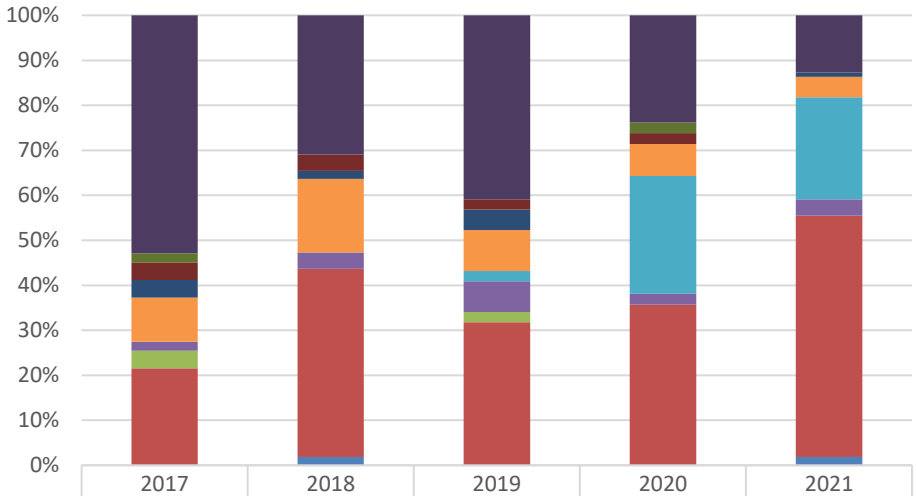


	Education	Financial	Government	Health	Hospitality	Other	Retail
Consumers Affected	195,137	3,082,107	7,765	1,127,327	167,673	916,137	542,086
# Type of Breach	23	77	8	42	31	59	62

Figure 3

From January 2017 through December 2021, Education providers reported twenty-three security breaches affecting 195,137 residents. Financial service providers reported seventy-seven security breaches affecting over 3 million residents. Governmental entities reported eight security breaches affecting 7,765 South Carolina residents. The healthcare industry reported forty-two security breaches that affected just over 1.1 million residents. The hospitality industry reported thirty-one breaches, which affected 167,673 residents. The retail industry reported sixty-two security breaches that affected 542,086 residents. Other industries falling outside these six main sectors filed fifty-nine notices affecting 916,137 residents.

Types of Breaches
January 2017 – December 2021



	2017	2018	2019	2020	2021
Hacking - malicious attacks on computer networks	27	17	18	10	14
Improper disposal of documents - personal data left in documents deposited in publicly accessible garbage bin	1			1	
Loss of IT equipment - misplaced or stolen equipment - laptops, USB sticks, etc.	2	2	1	1	
Mailing - distribution of a letter in the mail or an email to an incorrect address that includes personal data	2	1	2		1
Phishing Attack	5	9	4	3	5
Ransomware Attack			1	11	25
Technical error - unforeseen complication in an IT system exposing data to outside parties	1	2	3	1	4
Theft - data in the form of documents, electronically stored data, etc. that is stolen	2		1		
Unauthorized access - employee or outside party improperly attained access to system	11	23	14	15	59
Unauthorized disclosure - e.g. distributing personal data on peer-to-peer networks		1			2

Figure 4

From 2017 to 2021, the most prevalent types of breaches have been unauthorized access (122) and hacking (86). These two types of breaches represent 69% of the total number reported. SCDCA has received thirty-seven due to ransomware attacks; twenty-six due to phishing attacks; eleven caused by an unforeseen technical error; six due to mailing errors; six due to a loss of IT equipment; three due to theft; three caused by unauthorized disclosure; and two breach reports due to the improper disposal of documents.

In Depth Look at the Types of Breaches in 2021

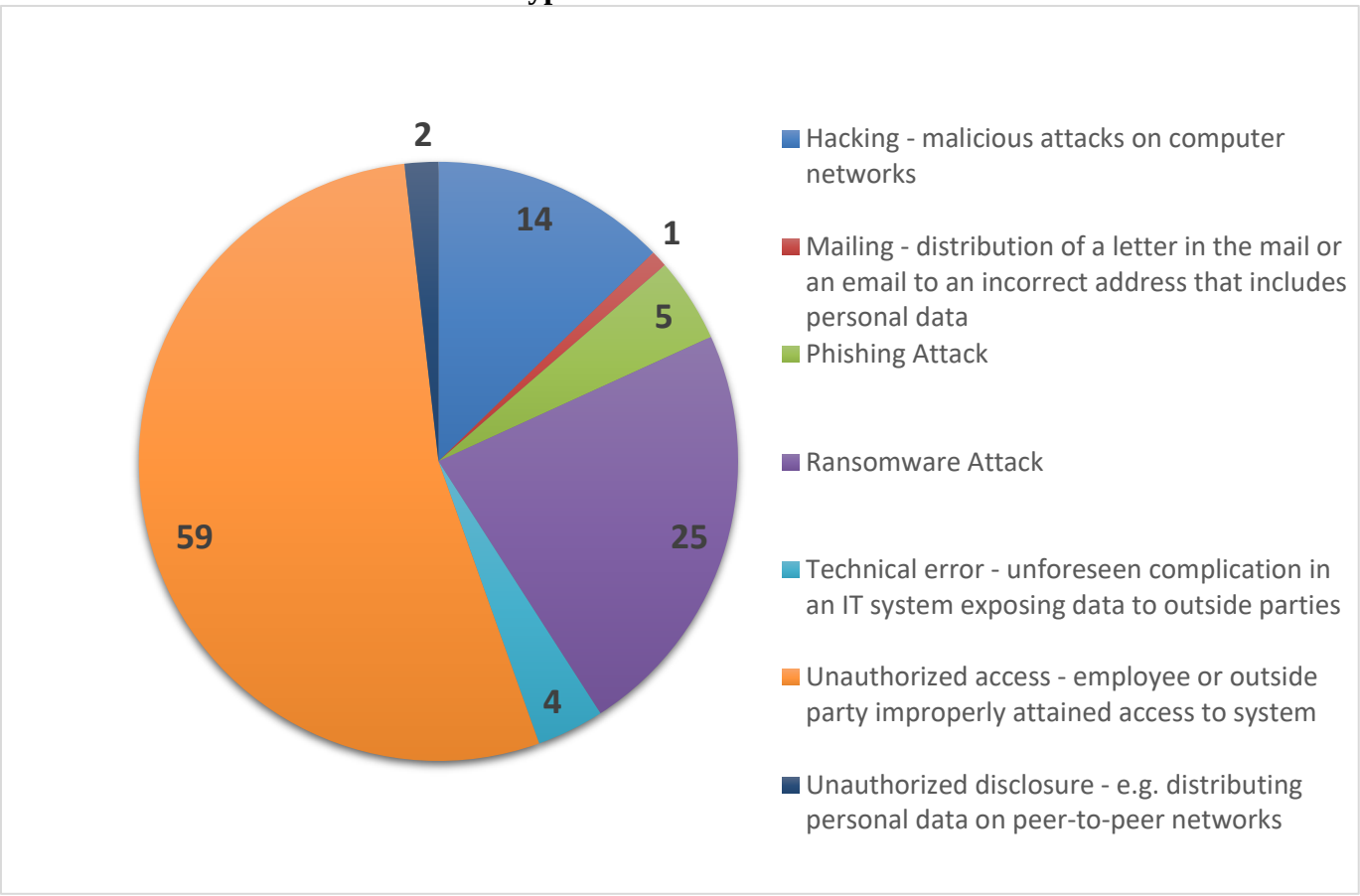
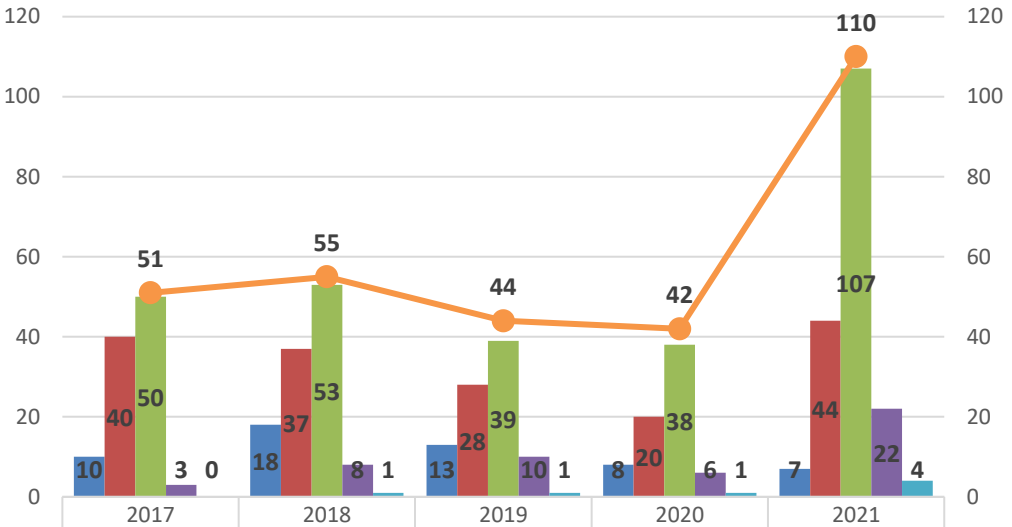


Figure 5

In 2021, SCDCA received fifty-nine security breach notices due to general unauthorized access to PII, representing 53.6% of the total breaches reported for the year. Twenty-five breaches (22.7% of total) were due to ransomware attacks. Fourteen reports of breaches (12.7%) were due to hacking. The remaining 11% of the total breaches reported were five security breaches due to phishing attacks; four breaches due to a technical error; two breaches were caused by unauthorized disclosure, e.g., distributing personal data on peer-to-peer networks; and one security breach reported was due to distribution of a letter in the mail or an email to an incorrect address that includes personal data.

Most notably, the number of unauthorized access breaches nearly quadrupled in 2021 (59) compared to 2020 (15). Ransomware breaches more than doubled in 2021 (25) compared to 2020 (11). The number of hacking breaches increased slightly from 10 (2020) to 14 (2021). Phishing attacks increased from 3 (2020) to 5 (2021) and technical errors increased from 1 (2020) to 4 (2021. There were two unauthorized disclosure breaches and one mailing error breach reported in 2021, although no breaches were reported in 2020 for these types.

Types of Data Breached
January 2017 – December 2021



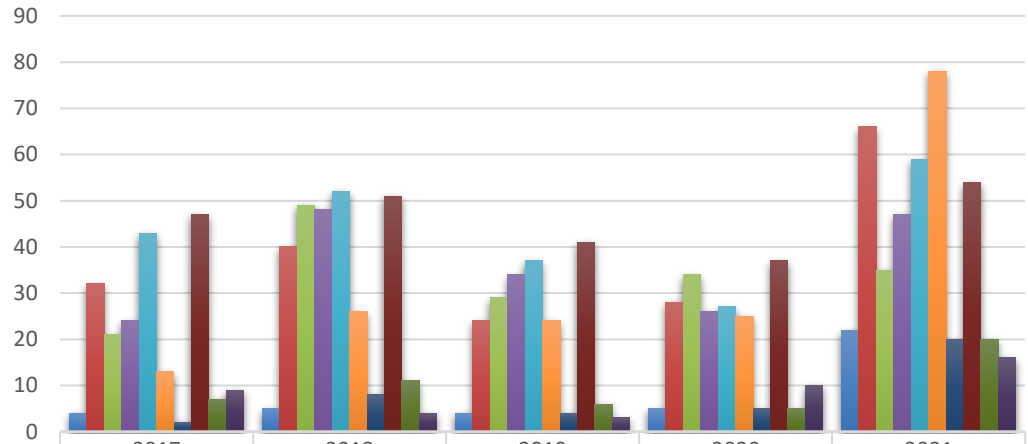
	2017	2018	2019	2020	2021
Credential Data (personal email, account username/password)	10	18	13	8	7
Financial Data (credit/debit card numbers, income, financial transactions, bank statements, etc.)	40	37	28	20	44
Personal Data (SSN/Tax ID, full name, address, driver's license no.)	50	53	39	38	107
Protected Health Data (diagnoses, treatment info, test results, etc.)	3	8	10	6	22
Other	0	1	1	1	4
Breaches Per Year	51	55	44	42	110

Figure 6

From 2017 to 2021, SCDCA received 302 reports of security breaches. Of those, 287 (95%) of reported breaches involved the exposure of protected personal data; 169 (56%) involved financial data; 56 (18.5%) involved credential data; 49 (16.2%) involved protected health data; and seven (2.3%) involved other types of potentially sensitive information, such as location data and academic history.[2] Notably, for 2017 to 2020, more breaches affected credential data than protected health data. In 2021, however, more breaches affected protected health data (20%) than credential data (6.4%).

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

Remediation Steps Taken by Reporting Organizations
January 2017 – December 2021



	2017	2018	2019	2020	2021
Change business network passwords	4	5	4	5	22
Credit monitoring services offered to affected consumers	32	40	24	28	66
Established call center for consumers	21	49	29	34	35
Fix data vulnerability issue(s)	24	48	34	26	47
Full assessment of security measures	43	52	37	27	59
Implement additional security safeguards	13	26	24	25	78
Implement Policies & Procedures	2	8	4	5	20
Provide consumer education on identity theft and fraud	47	51	41	37	54
Require users to change passwords	7	11	6	5	20
Other	9	4	3	10	16

Figure 7

In 2017, 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.[3] For the 302 breaches reported 2017–2021, 76.2% provided consumer education on identity theft and fraud; 72.2% initiated a full assessment of their security measures; 63% offered free credit monitoring services to affected consumers; 59.3% fixed data vulnerability issues; 55.6% established a dedicated call center for affected consumers; 55% implemented additional security safeguards; 16.2% required users to change their passwords; 13.2% changed their business network passwords; 12.9% implemented policies and procedures related to protecting sensitive data; and 13.9% 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. One of the most significant changes in 2021 is the increase in number of breaches where organizations implemented additional security safeguards (71% in 2021) from the previous 5-year average of 46%.

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

For those South Carolina residents 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.