




# County of Fairfax, Virginia

## MEMORANDUM

**DATE:** March 8, 2022

**TO:** Consumer Protection Commission

**FROM:** Rebecca L. Makely, Acting Director   
Department of Cable and Consumer Services

**SUBJECT:** Consumer Protection Commission Meeting for March 15, 2022

Please find attached the Consumer Protection Commission meeting packet. The next scheduled meeting is **Tuesday, March 15, 2022, 7:30 p.m.** This meeting will be held via a video connection due to the COVID-19 pandemic.

To join the meeting:

[Click here to join the meeting](#)

Audio-only participation:

Dial: 571-429-5982

Enter Conference ID: 449 555 09#

Please RSVP with your attendance to Susan Jones by COB on Monday, March 14, 2022, at [Susan.Jones@fairfaxcounty.gov](mailto:Susan.Jones@fairfaxcounty.gov) or 703-324-5877.

Enclosures

cc: Ellicia Seard-McCormick, Deputy County Executive

Susan C. Jones, Consumer Specialist III  
Department of Cable and Consumer Services



**FAIRFAX COUNTY  
CONSUMER PROTECTION COMMISSION  
March 15, 2022 AGENDA**

Call to Order by the Chairperson (7:30 PM)

Electronic Meeting Motions

Minutes

- Approval of the draft February 15, 2022, meeting minutes

Report of the Chairperson

Report of the Director

Commission Matters

Old Business

New Business

- 2022 Elections

General Interest

- Consumer Protection Commission Calendar
- Consumer Protection Commission Membership
- Consumer Affairs Statistics
- Community Outreach
- Consumer Resources

## **Minutes of the Fairfax County Consumer Protection Commission**

February 15, 2022

7:30 PM  
Video Meeting  
Chairperson Fee, presiding

Attendance:

Commissioners: Belkowitz, Callender, Fee,  
Gulakowski, Kirk, Kratovil, Roark, Rosier,  
Springer, Svab

Absent:

Commissioners: Hargraves

Staff:

Rebecca L. Makely, Acting Director  
Cable and Consumer Services  
Susan C. Jones, Branch Chief  
Consumer Affairs Branch  
Prescott Barbash, Consumer Specialist I  
Consumer Affairs Branch

The meeting was called to order at 7:30 PM by Chairperson Fee.

### **Quorum, Location, and Audibility of Member's Voices**

Chairperson Fee conducted a Roll Call to verify that a quorum of members were participating; and that each member's voice was clear, audible, and at appropriate volume for all of the other members; and the location from which member was participating. The roll call was as follows:

Conduct Roll Call:

Chairperson Fee, Burke  
Commissioner Belkowitz, Fairfax Station  
Commissioner Callender, Great Falls  
Commissioner Gulakowski, Burke  
Commissioner Hargraves, Absent  
Commissioner Kirk, Falls Church  
Commissioner Kratovil, Mount Vernon  
Commissioner Roark, Lorton  
Commissioner Rosier, Great Falls  
Commissioner Springer, Oakton  
Commissioner Svab, Fairfax

Chairperson Fee passed the virtual gavel to Vice Chairperson Gulakowski. A motion was made by Chairperson Fee that each member's voice was adequately heard by each member of the Consumer Protection Commission (Commission.) This motion was seconded by Commissioners Callender, Springer, and Svab. This motion passed 10-0-0.

### **Need for an Electronic Meeting**

A motion was made by Chairperson Fee that the State of Emergency caused by the COVID-19 pandemic made it unsafe for the Commission to physically assemble and unsafe for the public to physically attend any such meeting, and that as such, FOIA's usual procedures, which require the physical assembly of the Commission and the physical presence of the public, could not be implemented safely or practically. Chairperson Fee further moved that the Commission conduct the meeting electronically through a dedicated audio-conferencing line, and that the public access the meeting by calling 571-459-5982 and entering access code 695 758 847#. The motion was seconded by Commissioner Kirk. The motion passed 10-0-0.

### **Need to Dispense with FOIA's Usual Procedures to Assure Continuity in Government/Continue Operations**

A motion was made by Chairperson Fee that all of the matters addressed on the agenda addressed the Emergency itself, were necessary for continuity in Fairfax County government, and/or were statutorily required or necessary to continue operations and the discharge of the Commission's lawful purposes, duties, and responsibilities. This motion was seconded by Commissioner Kirk. The motion was passed 10-0-0.

### **Minutes**

The minutes for the January 18, 2021, meeting were approved without objection.

### **Report of the Chairperson**

Chairperson Fee had no matters to bring before the Commission.

### **Report of the Director**

Acting Director Makely had no matters to bring before the Commission.

### **Commission Matters**

Commissioner Belkowitz spoke of an issue with identity theft. He contacted Bank of America who recommended he contact the Post Office for a possible change of address. The next day he received a card from the Post Office to confirm his fraudulent change of address to a location in New York.

Commissioner Callender had no matters to bring before the Commission.

Commissioner Gulakowski expressed difficulty with Teams meeting invite.

A discussion ensued on using other platforms to reach consumers of all ages like Nextdoor, news stations, outreach events, and whether Commissioners can comment on platforms when offering resources provided by the County.

Commissioner Kirk mentioned continued issues with porch pirates taking packages from consumer's homes and that consumers need to consider other options like delivering to a neighbor's house.

Commissioner Kratovil inquired on the status of edits to Chapter 28.1 massage ordinance and CPC involvement in the process. Commissioner Kratovil provided an overview of what led to this discussion and his review of Chapter 28.1 that pertains to the appeal process.

Acting Director Makely advised the Commission that she entered Commissioner Kratovil's redline changes into a draft working copy of Chapter 28.1. She will send the information for their review. Acting Director Makely also stated a memo to the Board was sent late Friday night pertaining to Illicit Massage Establishments and Chapter 28.1. She will review and discuss with Deputy County Executive Seard-McCormick and will review item at the next meeting.

Commissioner Roark had no matters to bring before the Commission.

Commissioner Rosier had no matters to bring before the Commission.

Commissioner Springer had no matters to bring before the Commission.

Commissioner Svab inquired about the removal of the COVID testing site from the Government Center Parking Lot B. Acting Director Makely explained the Virginia Department of Health scheduled the community testing center for 30 days and which has now ended. Acting Director Makely reminded Commissioners that vaccinations were still available with appointment inside the Government Center.

Chairperson Fee spoke about identity theft with a credit union and card used to charge \$100. Chairperson Fee was unhappy with the response with the credit union and filed a complaint with the National Credit Union Administration. Chairperson Fee also mentioned the recent towing legislation that had failed to be approved.

### **Old Business**

Chapter 28.1 Massage Therapy, Establishments and Services

### **New Business**

**1. Consumer Affairs 101-** Susan Jones, Branch Manager, Consumer Affairs provided an overview of Consumer Affairs services and resources. Commissioners were reminded that March 7-11 is National Consumer Protection Week.

Chairperson Fee made the motion to adjourn. Commissioner Kirk seconded the motion.

The meeting adjourned at 8:43 PM.

# CPC Calendar

**Consumer Protection Commission**  
2022 Planning Calendar  
March 15, 2022

- January 18
  - Nominations of Officers
  - 2022 Meeting Calendar
  - 2022 Items of Interest
  
- February 15
  - Consumer Affairs 101
  
- March 15
  - 2022 Elections
  
- April 19
  - 2022 Legislative Review
  
- May 17
  - Regulation and Licensing 101
  
- June 21
  - Police Civilian Review Panel Presentation
  
- July 19
  - FY 2022 Annual Report
  
- August 16
  - Community-wide Energy and Climate Action Plan (CECAP)
  
- September 20
  - Silver Shield Task Force Presentation
  
- October 18
  - Bitcoin/Cryptocurrency
  
- November 15
  - Nominations of Officers
  
- December 20
  -

# CPC Membership



**Name**

**Staff**

Harold G. Belkowitz  
*Appt. Expires 7/31/2024*

Wes Callender  
*Appt. Expires 7/31/2024*

John Fee (Chairperson)  
*Appt. Expires 7/31/2024*

Denis Gulakowski  
(Vice-Chairperson)  
*Appt. Expires 7/31/2024*

Dirck A. Hargraves  
*Appt. Expires 7/31/2023*

Dennis D. Kirk  
*Appt. Expires 7/31/2022*

Jason J. Kratovil  
*Appt. Expires: 7/31/2024*

Michael J. Roark  
*Appt. Expires 7/31/2023*

Jacqueline Rosier (Secretary)  
*Appt. Expires 7/31/2022*

Dr. Maurice B. Springer  
*Appt. Expires 7/31/2024*

Mr. Paul Svab  
*Appt. Expires 7/31/2024*

Rebecca L. Makely, Acting Director  
Department of Cable and Consumer Services  
703-324-5947  
[rebecca.makely@fairfaxcounty.gov](mailto:rebecca.makely@fairfaxcounty.gov)

Susan Jones, Chief  
Consumer Affairs Branch  
703-324-5877  
[susan.jones@fairfaxcounty.gov](mailto:susan.jones@fairfaxcounty.gov)

Main number: 703-222-8435  
Fax number: 703-653-1310

# CAB Statistics



**Consumer Affairs Branch**  
**Monthly Summary - All Activities**  
**February 2022**

	Current Month		Fiscal Year-to-Date		Prior Fiscal YTD	
<b>Cases Received</b>	72		725		610	
<b>Cases Closed</b>	49		503		530	
Favorable	28	57%	283	56%	299	56%
Unfavorable	3	6%	51	10%	42	8%
Invalid	0	0%	18	4%	20	4%
Other	18	37%	151	30%	169	32%
<b>Total</b>	49	100%	503	100%	530	100%
Advice Inquires	263		2564		3200	
Case Inquires over 90+days	17		144		149	
<b>Amount Received</b>	\$70,680.00		\$382,225.00		\$309,313.00	

**CLOSED COMPLAINT CATEGORIES**

	FISCAL YEAR-TO-DATE	% FYTD	PRIOR FISCAL YTD	% PRIOR FYTD
Tenant Landlord		22%	Cable Television (Regulated)	24%
Automotive - Services		14%	Tenant Landlord	22%
Housing - Services		12%	Housing - Services	9%
Professional Services		5%	Automotive - Towing	7%
Retail		5%	Automotive - Services	6%
Other		42%	Other	32%

# Community Outreach

## Outreach Event Calendar March 2022

DATE	EVENT	LOCATION	# of Guests	Event Time	Staff
3/7/2022	<b>NCPW:</b> <b>Consumer Connection:</b> Mail Fraud	Fairfax County Government 12000 Government Center Pkwy Fairfax, VA		10:00 a.m. - 11:00 a.m.	SCJ
3/8/2022	<b>NCPW:</b> <b>Department of Treasury</b> Unclaimed Property	Virtual 101 N. 14th Street Richmond, VA		10:00 a.m. - 4:00 p.m.	
3/9/2022	<b>NCPW:</b> Is It a Charity or Is It a Scam	George Mason Regional Library (Zoom) 7001 Little River Turnpike Annandale, VA		7:00 p.m. -8:00 p.m.	MP
3/9/2022	<b>NCPW:</b> Who's Watching Whom? Your Smart TV and Your Privacy	Fairfax County Government 12000 Government Center Pkwy Fairfax, VA		1:00 p.m. - 2:00 p.m.	CPRD
3/10/2022	<b>NCPW:</b> Housing Fair	George Mason University Johnson Center 4400 University Drive Fairfax, VA		11:00 a.m. - 1:00 p.m.	MP
3/10/2022	<b>NCPW:</b> Scam Presentation	Financial Empowerment Center (Virtual) 8350 Richmond Highway Alexandria, VA		6:30 p.m. - 7:30 p.m.	PNB
3/11/2022	<b>NCPW:</b> Consumer Affairs 101	Fairfax County Government Center (Virtual) 12000 Government Center Parkway Fairfax, VA		12:00 p.m. - 12:30 p.m.	SCJ
3/16/2022	<b>Is it a Charity or Is it a Scam</b>	Braddock District Council (Zoom) 9002 Burke Lake Road Burke, VA		1:00 p.m. - 2:00 p.m.	MP

# Outreach Event Calendar

## April 2022

DATE	EVENT	LOCATION	# of Guests	Event Time	Staff
4/23/2022	Culmore Community Day 2022	Woodrow Wilson Library 6101 Knollwood Drive Falls Church, VA		10:00 a.m. - 2:00 p.m.	SCJ
4/26/2022	6th Fraud Prevention & Awareness Expo	Greenspring Hunters Crossing Conference Center 7430 Spring Village Drive Springfield, VA		11:00 a.m. - 2:00 p.m.	SCJ/ BEO

# Consumer Resources

## **Resource Items**

### **Fairfax County Department of Cable and Consumer Services**

<https://www.fairfaxcounty.gov/cableconsumer>

### **Fairfax County Consumer Affairs**

<https://www.fairfaxcounty.gov/cableconsumer/csd/consumer>

### **Fairfax County Consumer Affairs Facebook**

<https://www.facebook.com/fairfaxcountyconsumer/>

### **Fairfax County Coronavirus (COVID-19) Updates**

[Fairfaxcounty.gov/covid19/](https://www.fairfaxcounty.gov/covid19/)

### **Ways to Stay Informed About Coronavirus (COVID-19)**

<https://fairfaxcountyemergency.wpcomstaging.com/>

### **Ways to Donate and Help During COVID-19**

<https://fairfaxcountyemergency.wpcomstaging.com/2020/03/25/ways-to-donate-and-help-during-covid-19/>

### **What to Know About Tenant-Landlord Rights During COVID-19**

<https://fairfaxcountyemergency.wpcomstaging.com/2020/11/17/what-to-know-about-tenant-landlord-rights-during-covid-19/>

### **DCCS Operating Status**

<https://www.fairfaxcounty.gov/cableconsumer/status>

### ***Your Community, You're Connected: Association Communication (March 7, 2022)***

[Your Community, You're Connected | Cable and Consumer Services \(fairfaxcounty.gov\)](https://www.fairfaxcounty.gov/cableconsumer/status)

### ***Consumer Connection: Telemarketing Fraud (March 7, 2022)***

<https://fb.watch/bC2c0U1XtZ/>

## **Information Items**

### **Cybercriminals Tampering with QR Codes to Steal Victim Funds**

The FBI is issuing this announcement to raise awareness of malicious Quick Response (QR) codes. Cybercriminals are tampering with QR codes to redirect victims to malicious sites that steal login and financial information. [\[More\]](#)

### **Spot the Red Flags of Elder Financial Abuse**

In the wake of the coronavirus pandemic, many older adults are more socially isolated than ever — and thus more vulnerable to being financially victimized. [\[More\]](#)

### **Consumers lost \$5.8 billion to fraud last year — up 70% over 2020**

American consumers reported losing more than \$5.8 billion to fraud last year, up from \$3.4 billion in 2020 (an increase of more than 70%), the Federal Trade Commission said Tuesday. [\[More\]](#)



# **Cybercriminals Tampering with QR Codes to Steal Victim Funds**

**January 18, 2022 PSA- Alert Number  
I-011822-PSA**

The FBI is issuing this announcement to raise awareness of malicious Quick Response (QR) codes. Cybercriminals are tampering with QR codes to redirect victims to malicious sites that steal login and financial information.

A QR code is a square barcode that a smartphone camera can scan and read to provide quick access to a website, to prompt the download of an application, and to direct payment to an intended recipient. Businesses use QR codes legitimately to provide convenient contactless access and have used them more frequently during the COVID-19 pandemic. However, cybercriminals are taking advantage of this technology by directing QR code scans to malicious sites to steal victim data, embedding malware to gain access to the victim's device, and redirecting payment for cybercriminal use.

Cybercriminals tamper with both digital and physical QR codes to replace legitimate codes with malicious codes. A victim scans what they think to be a legitimate code but the tampered code directs victims to a malicious site, which prompts them to enter login and financial information. Access to this victim information gives the cybercriminal the ability to potentially steal funds through victim accounts.

Malicious QR codes may also contain embedded malware, allowing a criminal to gain access to the victim's mobile device and steal the victim's location as well as personal and financial information. The cybercriminal can leverage the stolen financial information to withdraw funds from victim accounts.

Businesses and individuals also use QR codes to facilitate payment. A business provides customers with a QR code directing them to a site where they can complete a payment transaction. However, a cybercriminal can replace the intended code with a tampered QR code and redirect the sender's payment for cybercriminal use.

While QR codes are not malicious in nature, it is important to practice caution when entering financial information as well as providing payment through a site navigated to through a QR code. Law enforcement cannot guarantee the recovery of lost funds after transfer.

## **TIPS TO PROTECT YOURSELF:**

- Once you scan a QR code, check the URL to make sure it is the intended site and looks authentic. A malicious domain name may be similar to the intended URL but with typos or a misplaced letter.
- Practice caution when entering login, personal, or financial information from a site navigated to from a QR code.
- If scanning a physical QR code, ensure the code has not been tampered with, such as with a sticker placed on top of the original code.
- Do not download an app from a QR code. Use your phone's app store for a safer download.

- If you receive an email stating a payment failed from a company you recently made a purchase with and the company states you can only complete the payment through a QR code, call the company to verify. Locate the company's phone number through a trusted site rather than a number provided in the email.
- Do not download a QR code scanner app. This increases your risk of downloading malware onto your device. Most phones have a built-in scanner through the camera app.
- If you receive a QR code that you believe to be from someone you know, reach out to them through a known number or address to verify that the code is from them.
- Avoid making payments through a site navigated to from a QR code. Instead, manually enter a known and trusted URL to complete the payment.

If you believe you have been a victim of stolen funds from a tampered QR code, report the fraud to your local FBI field office at [www.fbi.gov/contact-us/field-offices](http://www.fbi.gov/contact-us/field-offices). The FBI also encourages victims to report fraudulent or suspicious activities to the FBI Internet Crime Complaint Center at [www.ic3.gov](http://www.ic3.gov).

# Spot the Red Flags of Elder Financial Abuse

Unusual transactions and new ‘friends’ could be signs an older loved one is being exploited

by Lynnette Khalfani-Cox, [AARP](#), February 28, 2022

In the wake of the coronavirus pandemic, many older adults are more socially isolated than ever — and thus more vulnerable to being financially victimized.

Elder financial exploitation extends far beyond random con artists bombarding older adults with robocalls and phishing emails. According to the National Adult Protective Services Association, the “vast majority” of cases reported to its member agencies involve people the victim knows, including relatives, caregivers, neighbors and friends.

Financial exploitation can range from stealing someone’s Social Security check to forging financial documents to misappropriating cash, jewelry and other assets. Such financial fraud costs older adults at least \$36.5 billion annually, the National Council on Aging estimates.

Here are telltale signs and circumstances that can help you spot elder financial abuse — and possibly prevent it from happening to you or someone you love.

## Unusual financial activity

A major red flag of potential financial abuse is “unexplained activity in an older person’s accounts,” says Stephanie Genkin, a certified financial planner in New York.

Inquire about large withdrawals and unpaid bills to make sure there are no questionable credit card charges. Stop any bank transfers or recurring transactions the account holder does not recall making. It’s not uncommon for older individuals to forget things from time to time, but major financial dealings they have no memory of requesting or authorizing, or that they have difficulty explaining, should set off alarm bells.

Genkin suggests periodically reviewing an aging loved one’s bank and credit card statements with them to help guard against fraud. If possible, create a transparent system that allows both of you to monitor financial activity and perform basic record-keeping, and keep the lines of communication over money matters open.

## **New ‘friends’ or helpers**

Individuals who live alone are particularly susceptible to financial exploitation. Wrongdoers can more readily hide their misdeeds if no one else is around.

Experts caution that perpetrators of financial abuse, especially new acquaintances, frequently try to box out others and limit relatives’ contact with a vulnerable, older adult.

“Isolation is the number one tip-off,” says Michael McGuire, an attorney and president of the California Elder Law Center.

“It can be very subtle,” he adds. “A new ‘friend’ may try to cut off the family from getting access to the senior. All of a sudden, this ‘friend’ is saying: ‘They’re not available, they’re taking a nap or they’re not feeling well right now. I’ll have them call you back.’ And then they never do.”

Be especially wary of newcomers who insinuate themselves into an older person’s life in a way that makes the new associate indispensable in the eyes of the victim. Many schemers are initially incredibly helpful, McGuire says, “taking the senior to the store or their doctor’s appointments or restaurants — and, most importantly, they’re running them over to the bank.”

## **Cognitive decline or loss of financial acumen**

If an older person has known cognitive impairments such as Alzheimer’s or dementia or is beginning to show a loss of financial acumen, a designated family member or other trusted individual may need to immediately step in to help.

“Once a decline starts, it can happen very quickly,” Genkin says.

McGuire says unscrupulous family members, neighbors or friends may try to exert influence over people with cognitive issues. “With dementia, there’s a phenomenon that often occurs that whoever is the person sitting in front of the senior sort of wins the day” and can persuade the older adult to take financial actions they ordinarily wouldn’t, McGuire says.

Financial fraud can easily occur when a third party has access to an older adult’s sensitive private data, such as account numbers, passwords or Social Security number. Many older folks do need help with money management tasks, from simple bill paying to buying groceries, but their financial details should be closely guarded and only provided when necessary to known, trusted individuals.

## **Mobility or frailty issues**

Even those without cognitive impairments may be susceptible to financial abuse if they have physical disabilities or other issues that prevent them from driving or otherwise getting around.

For instance, older people with mobility issues who can't go to the bank on their own, or who aren't good with computers, may not have the physical ability or the know-how to do remote banking. They may have to rely on another person to handle routine transactions, such as deposits, withdrawals or transfers.

Genkin says she recently recommended to a client in his 80s and his relatives that they set up automatic bill pay for the client's cellphone, interest service and utilities. People with mental or physical impairments "shouldn't be left to figure out how to pay their own bills," she says.

She also highlights another consideration for caregivers: the role of outsiders in an older person's home.

"The pandemic has taken a toll on a lot of people," Genkin notes. Many Gen Xers and younger boomers who checked in frequently with parents or grandparents before COVID may now be paying for or arranging various services for those aging relatives.

"Now there are all these helpers around: preparing meals, tidying up the house, getting prescriptions or running errands, and some of them want to be paid in cash," Genkin says.

If you or someone you know is being financially exploited, tell someone you trust, report it to Adult Protective Services in your state and notify your local police department for help. You can also contact the U.S. Justice Department's National Elder Fraud Hotline at 833-372-8311.

*Lynnette Khalfani-Cox is a personal finance expert, speaker and author of 15 money-management books, including the New York Times bestseller Zero Debt: The Ultimate Guide to Financial Freedom.*

# Consumers lost \$5.8 billion to fraud last year — up 70% over 2020

PUBLISHED TUE, FEB 22 2023 3:33 PM EST UPDATED TUE, FEB 22 2024 4:01 PM EST

Greg Iacurci@GREGIACURCI

## KEY POINTS

- Consumers reported losing more than \$5.8 billion to fraud in 2021, a 70% increase over the prior year, the Federal Trade Commission said Tuesday.
- Almost 2.8 million people filed a fraud complaint, an annual record.
- Imposter scams were most prevalent, but investment scams cost the typical victim the most money.

American consumers reported losing more than \$5.8 billion to fraud last year, up from \$3.4 billion in 2020 (an increase of more than 70%), the Federal Trade Commission said Tuesday.

Almost 2.8 million consumers filed a fraud report to the agency in 2021 — the highest number on record dating back to 2001, according to the FTC. About 25% of those scams led to a financial loss, with the typical person losing \$500.

The true toll is almost certainly higher since some incidents likely weren't reported to the agency.

Those figures also don't include reports of identity theft and other categories. More than 1.4 million Americans also reported being a victim of identity theft in 2021; another 1.5 million filed complaints related to "other" categories (including credit reporting companies failing to investigate disputed information, or debt collectors falsely representing the amount or status of debt). Both sums are annual records, according to the FTC.

Fraud has ballooned during the Covid-19 pandemic, as con artists have preyed on consumer fear and confusion. They peddled fake health products (such as hand sanitizer and masks) and used stolen data to file for unemployment and other benefits in victims' names, for example.

Imposter scams were the most prevalent form of fraud in 2021, accounting for more than a third of reports, the FTC said. The typical victim lost \$1,000.