



County of Fairfax, Virginia

MEMORANDUM

DATE: March 14, 2023

TO: Consumer Protection Commission

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

SUBJECT: Consumer Protection Commission Meeting for March 21, 2023

Please find attached the Consumer Protection Commission meeting packet. The next scheduled meeting is **Tuesday, March 21, 2023, at 7:30 p.m. in Conference Room 232** of the Government Center, 12000 Government Center Parkway, Fairfax, Virginia.

Please RSVP with your attendance to Susan Jones by COB on Monday, March 20, 2023, at 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 21, 2023 AGENDA**

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

Remote Participation Motions

Minutes

- Approval of the draft February 21, 2023, meeting minutes

Report of the Chairperson

Report of the Director

Commissioner Matters

Old Business

New Business

- Request to Authorize Advertisement of a Public Hearing

General Interest

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

Minutes of the Fairfax County Consumer Protection Commission

February 21, 2023

7:30 PM
Government Center
12000 Government Center Parkway
Fairfax, VA 22035
Vice Chairperson Gulakowski, presiding

Attendance:

Commissioners: Belkowitz, Gulakowski,
Freedenthal, Hargraves, Kirk, Kharat, Kratovil,
Roark, Rosier, Springer, Svab

Absent:

Commissioner: O'Savio

Staff:

Rebecca L. Makely, Director
Cable and Consumer Services
Susan C. Jones, Consumer Specialist III
Consumer Affairs Branch

Guest Speakers:

Allison Homer, Planner IV
Office of Environmental and Energy Coordination
Maya Dhavale, Senior Community Specialist
Office of Environmental and Energy Coordination

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

Minutes

Commissioner Springer made the motion to accept the minutes. Commissioner Freedenthal seconded the motion. The minutes for the January 17, 2023, meetings were approved unanimously, 9-0-0.

Report of the Chairperson

Vice Chairperson Gulakowski recognized former Chairperson Fee's dedication and service to the Consumer Protection Commission and Trespass Towing Advisory Board.

Vice Chairperson Gulakowski attended a second virtual meeting of the Howard County Consumer Affairs Advisory Board.

Vice Chairperson Gulakowski requested Commissioners respond to staff emails on attendance so a quorum can be determined.

Report of the Director

Director Makely stated the County Executive presented the [FY 2024 Advertised Budget](#) today. The BOS will host budget town meetings throughout the County. Budget hearings will be held in April along with a joint meeting with Fairfax County Public School Board. The budget will be approved May 9, 2023.

Director Makely provided the Commission with a copy and overview of the Virginia General Assembly 2023 Legislative Session bills that were reviewed by Department of Cable and Consumer Services.

Commissioner Matters

Commissioner Rosier had no matters to bring before the Commission.

Commissioner Svab had no matters to bring before the Commission.

Commissioner Springer had no matters to bring before the Commission.

Commissioner Kratovil inquired about Chapter 28.1. Director Makely indicated an upcoming meeting with Tom Arnold, Deputy County Executive for Safety and Security to discuss the proposed amendments made by the CPC.

Commissioner Kirk noted his thanks and appreciation for former Chairperson Fee's service.

Commissioner Belkowitz had no matters to bring before the Commission.

Commissioner Freedenthal mentioned he was part of the Senior Medicare Patrol and would like to present to the CPC information on Medicare at a future meeting. He also mentioned the pending opening of the new Fairfax County Animal Shelter and the upcoming new Franconia Governmental Center Groundbreaking.

Commissioner Kharat had no matters to bring before the Commission.

Commissioner Roark had no matters to bring before the Commission.

Old Business

There was no old business.

New Business

1. Resilient Fairfax and CECAP Presentation. Allison Homer and Maya Dhavale provided a presentation on the Community-wide Energy and Climate Action Plan (CECAP) in Fairfax County. They spoke about the development of the Office of Environmental and Energy Coordination (OEEC), functions of OEEC, interagency coordination, energy use and efficiency tracking, community programs and innovation, future climate plans, weather vs. climate, emissions reduction, CECAP current status, buildings and energy efficiency, energy supply, climate projections, vulnerabilities, strategy pillars, and implementation roadmaps.

A discussion ensued on the building code, power outages, utility lines, and solar panels.

2. Elections of Officers. Nominating Committee, Vice Chairperson Gulakowski provided the Slate of Candidates: Chairperson - Jason Kratovil
Vice Chairperson - Denis Gulakowski
Secretary - Jacqueline Rosier

Commissioner Hargraves made the motion to accept the report of the Nominating Committee. Commissioner Freedenthal seconded the motion. The motion passed unanimously, 11-0-0.

3. 2023 Items of Interest. Topics mentioned: Medicare Fraud by Commissioner Freedenthal, FCPD Community/traffic patrol (Blake Lane) by Commissioner Springer, TNC/Taxicab industry update by Commissioner Belkowitz, and Electrification/EV charging by Commissioner Hargraves.

4. CPC Meeting Time. Commissioner Svab requested a discussion to change the CPC meeting time from 7:30 p.m. to 5:00 p.m. Commissioner Hargraves made the motion to consider meeting at 5:00 p.m. Commissioner Belkowitz seconded the motion. A discussion ensued on commissioner and public availability. The motion failed, 0-11-0.

Commissioner Kirk made the motion to adjourn without objection. The meeting adjourned at 8:53 PM.

CPC Calendar

Consumer Protection Commission
2023 Planning Calendar
March 21, 2023

- January 17
 - Chapter 28.1
 - 2023 Meeting Calendar

- February 21
 - Resilient Fairfax and CECAP Presentation
 - Election of Officers
 - 2023 Items of Interest

- March 21
 - Authorization to Advertise Public Hearing

- April 18
 - Public Hearing on Proposed Amendments to Fairfax County Code Section 28.1

- May 16
 - 2023 Taxicab Biennial Determination Report

- June 20
 - Virginia Senior Medicare Patrol Presentation by Commissioner Freedenthal

- July 18
 - FY 2023 Annual Report

- August 15
 -

- September 19
 - Electrification/EV Charging Presentation

- October 17
 -

- November 21
 - Nomination of Officers

- December 19
 -

CPC Membership

Name

Staff

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

Rebecca L. Makely, Director
Department of Cable and Consumer Services
703-324-5947
rebecca.makely@fairfaxcounty.gov

VACANT

Chester J. Freedenthal
Appt. Expires 7/31/2024

Susan Jones, Consumer Specialist III
Consumer Affairs Branch
703-324-5877
susan.jones@fairfaxcounty.gov

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

Main number: 703-222-8435, TTY 711
Fax number: 703-653-1310
consumer@fairfaxcounty.gov

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

Pratik J. Kharat
Appt. Expires 7/31/2024

Dennis D. Kirk
Appt. Expires 7/31/2025

Jason J. Kratovil (Chairperson)
Appt. Expires 7/31/2024

Triston "Chase" O'Savio
Appt. Expires 7/31/2024

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

Jacqueline Rosier (Secretary)
Appt. Expires 7/31/2025

Maurice B. Springer
Appt. Expires 07/31/2024

Paul Svab
Appt. Expires 7/31/2024

Community Outreach

Outreach Event Calendar March 2023

DATE	EVENT	LOCATION	# of Guests	Event Time	Staff
3/6/2023	Virginia Department of Treasury Unclaimed Property (Virtual)	101 North 14th Street Richmond, VA	15	10:00 a.m. - 4:00 p.m.	SCJ
3/7/2023	Funeral Planning (Zoom)	Brain Injury Services 8136 Old Keene Mill Road Springfield, VA	10	10:00 a.m. - 11:00 a.m.	LY CH
3/9/2023	Consumer Affairs Booth	Fairfax County Government Center Fairfax, VA	28	8:00 a.m. - 12:30 p.m.	All Staff
3/9/2023	Consumer Affairs Day Welcome and Consumer Affairs 101	Fairfax County Board Auditorium Fairfax, VA	11	9:00 a.m. - 9:30 a.m.	RLM SCJ
3/9/2023	Tenant and Landlord Rights and Responsibilities	Fairfax County Board Auditorium Fairfax, VA	11	9:30 a.m. - 10:15 a.m.	MP SW
3/9/2023	Funeral Planning	Fairfax County Board Auditorium Fairfax, VA	13	10:30 a.m. - 11:15 p.m.	LY CH
3/9/2023	Scams	Fairfax County Board Auditorium Fairfax, VA	15	11:15 a.m. - 12:00 p.m.	PB AB
3/9/2023	Scams	McLean Police Station 1437 Balls Hill Road McLean, VA	22	7:00 p.m. - 8:00 p.m.	PB AB
3/10/2023	7th Slam the Scam Fraud Prevention & Awareness Expo	Greenspring 7430 Spring Village Drive Springfield, VA	80	11:00 a.m. - 2:00 p.m.	SCJ SW
3/20/2023	Consumer Knowledge	Annandale High School 4700 Medford Drive Annandale, VA		8:00 a.m. - 4:00 p.m.	MP LY
3/21/2023	Consumer Knowledge	Annandale High School 4700 Medford Drive Annandale, VA		8:00 a.m. - 4:00 p.m.	MP CH
3/21/2023	Scams	South County Church 7880 Backlick Road Springfield, VA		12:30 p.m. - 1:30 p.m.	AB

Outreach Event Calendar April 2023

DATE	EVENT	LOCATION	# of Guests	Event Time	Staff
4/1/2023	Northern Virginia Housing Expo	Dominion High School 21326 Augusta Drive Sterling, VA		10:00 a.m. - 3:00 p.m.	MP
4/11/2023	Spring Off-Campus Housing Fair	George Mason University 450 Rivanna River Way Fairfax, VA		11:00 a.m. - 3:00 p.m.	MP LY
4/11/2023	Scam Presentation	ExxonMobile Potomic Annuitants Club		12:00 p.m. - 1:00 p.m.	PB AB
4/17/2023	Consumer Knowledge	West Potomac High School 6500 Quander Road Alexandria, VA		8:00 a.m. - 4:00 p.m.	MP CH
4/18/2023	Consumer Knowledge	West Potomac High School 6500 Quander Road Alexandria, VA		8:00 a.m. - 4:00 p.m.	MP LY
4/20/2023	Consumer Connection	Fairfax County Consumer Affairs Facebook		11:00 a.m. - 11:15 a.m.	SCJ
4/29/2023	Scam Jam 2023	George Mason University 450 Rivanna River Way Fairfax, VA		9:00 a.m. - 12:00 p.m.	SCJ

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/>

Consumer Connection: National Consumer Protection Week (March 9, 2023)

Consumer Affair 101/Tenants and Landlords Rights and Responsibilities

<https://fb.watch/jeYiuQcN3Z/>

Funeral Planning https://fb.watch/jeYoFPE_Yr/

Common Scams <https://fb.watch/jeYdCwf7X8/>

Information Items

Chick-fil-A confirms accounts hacked in months-long “automated” attack ([more](#))

LastPass Hack: Engineer’s Failure to Update Plex Software Led to Massive Data Breach ([more](#))

Crypto investments scammers are targeting your community groups ([more](#))

Chick-fil-A confirms accounts hacked in months-long "automated" attack

By

Lawrence Abrams

March 2, 2023

04:00 PM



American fast food chain Chick-fil-A has confirmed that over 71,000 customers' accounts were breached in a months-long credential stuffing attack, allowing threat actors to use stored rewards balances and access personal information.

In January, [BleepingComputer](#) reported that Chick-fil-A had begun investigating what it described as "suspicious activity" on customers' accounts.

We are investigating suspicious activity on some customer accounts. We are committed to protecting customers' data and are working quickly to resolve the issue. [Learn more.](#) ✕



Order
Now



Chick-fil-A alert on website

At the time, Chick-fil-A set up a support page with information on what customers should do if they detect suspicious activity on their accounts.

This warning came after BleepingComputer emailed Chick-fil-A before Christmas about reports of Chick-fil-A user accounts being stolen in credential-stuffing attacks and sold online.

These accounts were sold for prices ranging from \$2 to \$200, depending on the rewards account balance and linked payment methods.

One Telegram channel seen by BleepingComputer showed people purchasing these accounts and then sharing pictures of their purchases made through these accounts.

Add to cart ✕

\$15

- To see more details visit: <https://plagueis13.github.io/>

CATEGORIES

FOOD HOT PRODUCTS

AVAILABLE OPTIONS

- Chick Fil A + Balance [\$50] - price: 7.5\$
- Chick Fil A + Balance [\$2000] - price: 200\$
- Chick Fil A + Balance [\$1000] - price: 100\$
- Chick Fil A + Balance [\$500] - price: 75\$
- Chick Fil A + Balance [\$400] - price: 60\$
- Chick Fil A + Balance [\$300] - price: 50\$
- Chick Fil A + Balance [\$200] - price: 40\$
- Chick Fil A + Balance [\$100] - price: 20\$
- Chick Fil A + Balance [\$50] - price: 7.5\$
- Chick Fil A + PayPal - price: 5\$
- Chick Fil A + American Express/Discover - price: 3\$
- Chick Fil A + Visa/Mastercard - price: 2\$

Chick-fil-A accounts for sale
Source: BleepingComputer

Chick-fil-A confirms credential stuffing attack

Today, Chick-fil-A confirmed our reporting in a security notice submitted to multiple Attorney General offices, stating that they suffered a credential stuffing attack between December 18th, 2022, and February 12th, 2023. This sustained attack allowed the threat actors to hack a total of 71,473 Chick-fil-A accounts.

"Following a careful investigation, we determined that unauthorized parties launched an automated attack against our website and mobile application between December 18, 2022 and February 12, 2023 using account credentials (e.g., email addresses and passwords) obtained from a third-party source.

Based on our investigation, we determined on February 12, 2023 that the unauthorized parties subsequently accessed information in your Chick-fil-A One account." - [Chick-fil-A notification](#).

The fast food chain is warning impacted customers that threat actors who accessed their account would have also had access to their personal information, including their name, email address, Chick-fil-A One membership number and mobile pay number, QR code, masked credit/debit card number, and the amount of Chick-fil-A credit (e.g., e-gift card balance) on your account (if any).

For some customers, the information may have included birthdays, phone numbers, physical addresses, and the last four digits of credit cards.

In response to the attack, Chick-fil-A forced customers to reset passwords, froze funds loaded into accounts, and removed any stored payment information from accounts.

Chick-fil-A also states that they restored Chick-fil-A One account balances and added rewards to impacted accounts as a way of apologizing.

As the accounts were breached using credentials exposed in other data breaches, impacted users must change their passwords at all sites they frequent, especially if they use the same Chick-fil-A password.

When resetting passwords, use a unique password for each site and store them in a password manager, like Bitwarden, so that they can be easily managed.

While there is no evidence that personal information was abused, impacted customers should also be on the lookout for potentially targeted phishing emails utilizing this information.

LastPass Hack: Engineer's Failure to Update Plex Software Led to Massive Data Breach

📅 Mar 07, 2023 📍 Ravie Lakshmanan Password Security / Software Update

The image shows the LastPass logo, which consists of the word "Last" in white and "Pass" in orange, set against a dark blue background.

The massive breach at LastPass was the result of one of its engineers failing to update Plex on their home computer, in what's a sobering reminder of the dangers of failing to keep software up-to-date.

The embattled password management service last week [revealed](#) how unidentified actors leveraged information stolen from an earlier incident that took place prior to August 12, 2022, along with details "available from a third-party data breach and a vulnerability in a third-party media software package to launch a coordinated second attack" between August and October 2022.

The intrusion ultimately enabled the adversary to steal partially encrypted password vault data and customer information.

The second attack specifically singled out one of the four DevOps engineers, targeting their home computer with a keylogger malware to obtain the credentials and breach the cloud storage environment.

This, in turn, is said to have been made possible by exploiting a nearly three-year-old now-patched flaw in Plex to achieve code execution on the engineer's computer, the streaming media service told The Hacker News in a statement.

The vulnerability in question is [CVE-2020-5741](#) (CVSS score: 7.2), a deserialization flaw impacting Plex Media Server on Windows that allows a remote, authenticated attacker to execute arbitrary Python code in the context of the current operating system user.

Security: Regarding CVE-2020-5741

■ Announcements server-windows security-notices



PlexSecurity Plex Employee

May '20

Hello,

We have recently been made aware of a security vulnerability related to Plex Media Server. This issue allowed an attacker with access to the server administrator's Plex account to upload a malicious file via the Camera Upload feature and have the media server execute it. This could be done by setting the server data directory to overlap with the content location for a library on which Camera Upload was enabled. This issue could not be exploited without first gaining access to the server's Plex account. This issue has been assigned [CVE-2020-5741](#) 317

Starting in Plex Media Server 1.19.3, we are mitigating this issue in the following ways:

- We have removed the ability to change the location of the server's data directory via the API. Windows users can still change the directory location via the advanced server settings in the Registry.
- We also have added additional checks in the Camera Upload feature that disallow uploads to sensitive locations within the server data directory.

In summary: An attacker who already had admin access to a Plex Media Server could abuse the Camera Upload feature to make the server execute malicious code. Upgrade Plex Media Server to version 1.19.3 or newer and be careful with access to your admin account.

Thanks,

Plex Security Team

"This issue allowed an attacker with access to the server administrator's Plex account to upload a malicious file via the Camera Upload feature and have the media server execute it," Plex [said](#) in an advisory released at the time.

The shortcoming, which was [discovered and reported](#) to Plex by Tenable in March 2020, was addressed by Plex in [version 1.19.3.2764](#) released on May 7, 2020. The current version of Plex Media Server is 1.31.1.6733.

"Unfortunately, the LastPass employee never upgraded their software to activate the patch," Plex said in a statement. "For reference, the version that addressed this exploit was roughly 75 versions ago."

Crypto investment scammers are targeting your community groups

Cristina Miranda
Consumer Education Specialist, FTC
March 8, 2023



Did someone offer a can't-miss investment opportunity?
Skip it. It's a scam.

Report investment scams:
ReportFraud.ftc.gov

 **FEDERAL TRADE COMMISSION**



Crypto investment talk is everywhere — even in your local community groups in real life or online. But scammers join these groups, too. Their mission? Gain the group's trust...and then exploit relationships and trick you into crypto investment scams. But how do you spot and avoid these scammers?

Scammers use common bonds to build trust. They might speak the same language as you, claim to be the same age, or pretend to share things in common like your religion, ethnicity, hobbies, or profession. Why? Because when they then offer crypto investment advice or help, they think you'll be more likely to listen. Once they start chatting with you, before long, they'll ask you for money to invest in crypto, make up a reason you need to send a payment in crypto, or both. But if you give it to them, the money or crypto will be gone.

The bottom line? [Crypto investing](#) comes with lots of risks, including [scams](#). To spot the scams:

- **Don't believe promises that you'll make money, get a big payout, or earn guaranteed returns.** Those are [signs of a scam](#). No one can guarantee crypto investment riches.

- **Ask online group moderators to remove people pushing crypto.** Or, if you're a group moderator, remove anyone offering advice or "help" with crypto investing to prevent scams.
- **Research before you invest.** Scammers are exploiting what people don't know about crypto. It pays to search online for the company or currency name with the words "review," "scam," or "complaint." Find out how it works and where your money is going. If you need help making investment decisions while avoiding fraud, visit [Investor.gov](https://www.investor.gov).

And remember, anyone who tells you to pay by [cryptocurrency](#), [wire transfer](#), or [gift card](#) is a scammer. If you pay, there's usually no way to get your money back.

Read more at [ftc.gov/cryptocurrency](https://www.ftc.gov/cryptocurrency). Need to report a cryptocurrency scam? Visit [Reportfraud.ftc.gov](https://www.reportfraud.ftc.gov).