Please include this correspondence in the agenda for the Council meeting on Tuesday, May 28th.

With thanks,
Susan Watson

---------- Forwarded message ---------
From: **Susan Watson** [redacted]
Date: Mon, 6 May 2024 at 09:05
Subject: The $ value of fraud in Canada increased by almost 50% from 2021 to 2023
To: Erin Caton <erin.caton@guelph.ca>, Michele Richardson <michele.richardson@guelph.ca>, Linda Busuttil <linda.busuttil@guelph.ca>, Carly Klassen <carly.klassen@guelph.ca>, Phil Allt <phil.allt@guelph.ca>, Dan Gibson <dan.gibson@guelph.ca>, Rodrigo Goller <rodrigo.goller@guelph.ca>, Christine Billings <christine.billings@guelph.ca>, Cathy Downer <cathy.downer@guelph.ca>, Leanne Caron <Leanne.Caron@guelph.ca>, Dominique O'Rourke <dominique.orourke@guelph.ca>, Cam Guthrie <Cam.Guthrie@guelph.ca>, Mayors Office <mayor@guelph.ca>, Ken Yee Chew <ken.chew@guelph.ca>, Clerks <clerks@guelph.ca>

Mayor Guthrie and Members of City Council:

It is essential that you weigh the threat environment in Canada in deliberating on the most secure methods of voting for the 2026 municipal election.

On the Canadian Anti-Fraud Centre website, they document that $123 million has been lost to fraud so far this year:
https://antifraudcentre-centreantifraude.ca/index-eng.htm

The dollar value of fraud in Canada increased by almost 50% from 2021 to 2023.

Fraud is becoming more sophisticated. These new tools can also be deployed for internet voting fraud and manipulation.

I would encourage you to read the one-page Executive Summary of the Canadian Anti-Fraud Centre 2022 annual report:

https://antifraudcentre-centreantifraude.ca/annual-reports-2022-rapports-annuels-eng.htm

Here are the key trends:

2022 was a significant year for Canadian fraud victimization and losses.
The CAFC observed four ongoing and overarching trends during this time:

1. *Fraud is leading to larger losses - In 2021, the CAFC observed approximately $383 million in reported victim losses. In 2022, this number drastically increased to $530.4 million Endnote1*
2. *Fraud is becoming more personal - The CAFC received many reports of fraudsters and cybercriminals openly threatening victims, and using explicit content and personal and financial information to extort victims and their families. Victims are not just losing money or information, but are also exposed to situations of psychological and emotional harm*
3. *Fraud and cybercrime are targeting every age demographic - Another mistaken assumption is that fraud only victimizes seniors and vulnerable populations. Although reports by individuals aged 60+ outnumbered all other age groups in 2021, there was a drastic shift in reporting by age range in 2022. All age demographics are becoming targeted by fraud in 2022. Younger age groups are increasingly being victimized by nuanced and age-specific forms of fraud*
4. *Fraud is enabled by easier access to personal information - With Canadians posting more personal or specific information on accessible sites like LinkedIn, Facebook, Instagram, and Twitter, fraud operations are using this public information to create targeted and more believable fraud scenarios. Fraudsters can learn about someone’s friend groups, work, career aspirations, hobbies and interests, and financial situations through these mediums. Information stolen through cybercrime can also be obtained by fraudsters. This trend leads to specific, advanced and believable fraud attempts, increasing the potential for victimization.*

Please include this correspondence in the agenda for Tuesday's meeting.

Thank you.

Susan

---------- Forwarded message ---------
From: **Susan Watson** [redacted]
Date: Thu, 23 May 2024 at 12:07
Subject: City of Toronto statement on Internet Voting for the 2026 municipal election
To: Erin Caton <erin.caton@guelph.ca>, Michele Richardson <michele.richardson@guelph.ca>, Linda Busuttil <linda.busuttil@guelph.ca>, Carly Klassen <carly.klassen@guelph.ca>, Phil Allt <phil.allt@guelph.ca>, Dan Gibson <dan.gibson@guelph.ca>, Rodrigo Goller <rodrigo.goller@guelph.ca>, Christine Billings <christine.billings@guelph.ca>, Cathy Downer <cathy.downer@guelph.ca>, Leanne Caron <Leanne.Caron@guelph.ca>, Dominique O'Rourke <dominique.orourke@guelph.ca>, Cam Guthrie <Cam.Guthrie@guelph.ca>, Mayors Office <mayor@guelph.ca>, Ken Yee Chew <ken.chew@guelph.ca>, Clerks <clerks@guelph.ca>
Cc: Stephen O'Brien <Stephen.OBrien@guelph.ca>, Dylan McMahon <Dylan.McMahon@guelph.ca>, Jennifer Slater <Jennifer.Slater@guelph.ca>, Carrie Murray-Sprague <Carrie.Murray@guelph.ca>, Samantha Osborn <Samantha.Osborn@guelph.ca>, <adam.fischer@guelph.ca>

Mayor Guthrie and Members of Council:

I think the statement below, which I received via email this morning from the City of Toronto Elections, City Clerk's Office, will be relevant to your deliberations on May 28th.

Toronto Elections asserts:

Currently, there is no Internet voting service that can guarantee security, ballot secrecy and vote integrity; therefore, Internet voting will not be an option for the 2026 election.

The motion as it stands is setting a task for the Clerk that is destined to fail. Mr. O'Brien expressed concerns that given the withdrawal of Dominion and Scytl as internet election vendors, there may not be any remaining vendors who meet basic standards. This statement from the City of Toronto, a highly resourced municipality, confirms this. Why would we waste tens of thousands of tax dollars going down this dead end when the outcome is a foregone conclusion?

Back in 2014, the City of Toronto commissioned a security review of three Internet Vendor proposals. The final recommendation was to proceed with none of them. That document was released via a Freedom of Information request and is available at this link:

https://verifiedvoting.org/wp-content/uploads/2020/07/Canada-2014-01543-security-report.pdf

Sincerely,
Susan Watson

---------- Forwarded message ---------
From: **Elections - City Clerks** <elections@toronto.ca>
Date: Thu, 23 May 2024 at 10:58
Subject: RE: Will the City of Toronto be offering internet voting for the 2026 municipal election

Hello Susan,

Thank you for contacting Toronto Elections. Internet voting was examined for the 2014 election and found not acceptable regarding privacy and security of the vote. Continued research has made it clear that the significant vulnerabilities and technical challenges identified in past staff reports remain innumerable and unresolved.

Currently, there is no Internet voting service that can guarantee security, ballot secrecy and vote integrity; therefore, Internet voting will not be an option for the 2026 election. Toronto Elections will continue to investigate Internet voting for future elections.

You can find more information in the following reports to City Council:

- https://www.toronto.ca/legdocs/mmis/2016/ex/bgrd/backgroundfile-98545.pdf
- https://www.toronto.ca/legdocs/mmis/2014/cc/bgrd/backgroundfile-71290.pdf
- https://www.toronto.ca/legdocs/mmis/2014/cc/bgrd/backgroundfile-66912.pdf

Warm Regards,

Toronto Elections

Toronto Elections

City Clerk's Office

100 Queen Street West, 1st Floor

Toronto ON M5H 2N2
O 416.338.1111

F 416.395.1300

www.toronto.ca/elections

TORONTO

Sent: Tuesday, May 21, 2024 4:36 PM
To: Clerk <clerk@toronto.ca>
Subject: [External Sender] Will the City of Toronto be offering internet voting for the 2026 municipal election?

To Whom It May Concern:

Will the City of Toronto be offering internet voting for the 2026 municipal election?

Please let me know.

With thanks,

Susan Watson

Please include this correspondence in the agenda for Tuesday's meeting.

Thank you.

Susan

---------- Forwarded message ---------
From: **Susan Watson** [redacted]
Date: Wed, 22 May 2024 at 12:39
Subject: How Internet Voting Hurts Our Democracy
To: Erin Caton <erin.caton@guelph.ca>, Michele Richardson <michele.richardson@guelph.ca>, Linda Busuttil <linda.busuttil@guelph.ca>, Carly Klassen <carly.klassen@guelph.ca>, Phil Allt <phil.allt@guelph.ca>, Dan Gibson <dan.gibson@guelph.ca>, Rodrigo Goller <rodrigo.goller@guelph.ca>, Christine Billings <christine.billings@guelph.ca>, Cathy Downer <cathy.downer@guelph.ca>, Leanne Caron <Leanne.Caron@guelph.ca>, Dominique O'Rourke <dominique.orourke@guelph.ca>, Cam Guthrie <Cam.Guthrie@guelph.ca>, Mayors Office <mayor@guelph.ca>, Ken Yee Chew <ken.chew@guelph.ca>, Clerks <clerks@guelph.ca>

Dear Mayor Guthrie and Members of Council:

"Verified Voting" is an American organization. They have one of the best FAQs I've seen on internet voting. I hope it will be helpful for your decision making.

Sincerely,
Susan Watson

https://verifiedvoting.org/internet-voting-faq/

What is "internet voting"?

"Internet voting" is often called "electronic ballot return" and means returning a voted ballot over the internet — including via mobile apps, email, fax, or via a website.

Is there any evidence that internet voting is secure?

No. Many credible cybersecurity experts warn that internet voting is unsafe and, if implemented, makes U.S. elections easy targets for attackers who seek to change election outcomes or sow distrust in our democracy. In its 2018 consensus report, Securing the Vote, the National Academies of Sciences, Engineering and Medicine stated bluntly:
At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed and in

place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.

Similarly, in the lead up to the 2020 General Election, the Department of Homeland Security and three other federal agencies told states and election officials that electronic ballot return "creates significant security risks to the confidentiality of ballot and voter data (e.g., voter privacy and ballot secrecy), integrity of the voted ballot, and availability of the system. We view electronic ballot return as high risk."

Does internet voting keep a voter's ballot private?

Every voter has the right to vote privately, but a voter's identity must also be confirmed to ensure no one else votes in their name. This combination of privacy and identification is impossible with current internet voting technology. Internet voting exposes voters to widespread privacy violations by taking advantage of the fact that online voters must transmit their names with their votes. These privacy violations compromise a voter's right to a private ballot.

Can election officials conduct an audit of an election if internet voting is the primary voting method?

Voter-verified paper ballots are considered the most secure way of voting. These paper ballots can be audited and recounted to confirm election results. In contrast, ballots cast via the internet cannot be meaningfully audited. Even if an election official prints an electronically received ballot, the voter never interacted with the printed copy and cannot verify it is correct, meaning the printout cannot reliably document voter intent.

What types of attacks threaten the security of votes cast over the internet?

No internet-connected system of any kind, let alone a voting system, is invulnerable to attack, whether the votes are transmitted by email, fax, a web portal, or via a mobile app. Vulnerabilities include:

- Voter authentication attacks (forged voter credentials)
- Malware on voters' devices (malicious code hidden in apps or software updates) that can modify votes undetectably
- Denial of service attacks (slowing or crashing the system by overwhelming it with traffic or taking advantage of a bug)
- Server penetration attacks (remote break-in and control of the election server)
- Spoofing attacks (directing voters to a fake voting website instead of the real one)
- Voter coercion through automated vote buying and selling schemes (payment in exchange for votes)

What makes internet voting less safe than everything else I do on the internet?

While voting from a phone might sound nice, current internet voting technology does not allow votes to be both verifiable and untraceable back to the individual voter. A jurisdiction could track a voted ballot back to the voter via an IP address, email address, or the submitted email attachment. This limitation is not a problem for services like mobile banking and e-commerce, where online transactions should be traceable to individuals. The security of the actual device that voters cast their votes on is also unknown. The voter's device may already be corrupted with malware or viruses that could tamper with a ballot, interfere with ballot transmission, or even spread that malware to the elections office computer that receives the online ballot.

Who regulates internet voting?

Unlike physical voting equipment, there are currently no federal standards, testing, or certification procedures to regulate internet voting systems.

But internet voting vendors say their systems are secure.

Vendors of online election systems have a strong interest in selling their products. Through their public relations, marketing, and lobbying efforts, they consistently downplay the inherent risks of internet voting. The fundamental threats to internet voting systems currently have no strong solutions. Click here to see studies and security assessments conducted on these systems.

What about blockchain?

Blockchain is marketed by internet voting vendors as an adequate solution to internet voting vulnerabilities, but votes stored on a blockchain are susceptible to tampering before they enter the blockchain. Blockchain technology is designed to keep information secure after it is received and cannot defend against the multitude of threats to that information before it enters the blockchain. Voters cannot verify their votes are entered into the blockchain correctly without compromising ballot secrecy. Recording ballots on a blockchain also risks ballot secrecy if encryption keys are not properly protected or software errors allow decryption of individual ballots.

What secure, accessible options are available for voters?

Every voter has the right to vote privately and anonymously, and know that their votes were counted as cast. With the right resources, jurisdictions can conduct elections safely and securely for all voters. Recommendations for making voting more accessible include:

- Sending an electronic blank ballot that a voter can mark, print, and verify with assistive technology and then print and return to the elections office via mail or at a drop box
- Making mail ballots more compatible with various assistive technologies
- Having ADA-compliant drop box locations and more inclusive policies for collecting and returning mail ballots on behalf of voters with disabilities
- Ensuring that accessible voting equipment is available and functioning at polling places

- Ensuring that all in-person polling locations are fully compliant with ADA requirements
- Making accessible voting equipment available curbside and even taking accessible equipment and/or printers to voters at their homes so they can vote privately and independently

More investment, research and collaboration is needed to develop better options for voters with disabilities that meet their needs while also protecting our elections and the ballot secrecy of the voter in ways that internet voting does not. Internet voting is often touted as a cure-all, but it poses its own issues with accessibility — even beyond security concerns. With security and disability rights groups working together, we can ensure every voter casts a private ballot with justified confidence that it will be counted as cast.

Dear Clerks:

Please include this correspondence in the agenda for Tuesday's meeting.

With thanks,
Susan

---------- Forwarded message ---------
From: **Susan Watson** [redacted]
Date: Mon, 6 May 2024 at 20:51
Subject: Recent American studies on internet voting
To: Erin Caton <erin.caton@guelph.ca>, Michele Richardson <michele.richardson@guelph.ca>, Linda Busuttil <linda.busuttil@guelph.ca>, Carly Klassen <carly.klassen@guelph.ca>, Phil Allt <phil.allt@guelph.ca>, Dan Gibson <dan.gibson@guelph.ca>, Rodrigo Goller <rodrigo.goller@guelph.ca>, Christine Billings <christine.billings@guelph.ca>, Cathy Downer <cathy.downer@guelph.ca>, Leanne Caron <Leanne.Caron@guelph.ca>, Dominique O'Rourke <dominique.orourke@guelph.ca>, Cam Guthrie <Cam.Guthrie@guelph.ca>, Mayors Office <mayor@guelph.ca>, Ken Yee Chew <ken.chew@guelph.ca>, Clerks <clerks@guelph.ca>

Mayor Guthrie and Members of Council:

A diverse range of American studies on internet voting are highlighted in a report produced by the American organization: "Verified Voting." ***"Casting Votes Safely: Examining Internet Voting's Dangers and Highlighting Safer Alternatives.":***
https://verifiedvoting.org/wp-content/uploads/2023/10/VerifiedVoting-CastingVotesSafely-2023-FIN.pdf

CONSENSUS STUDIES EXAMINING INTERNET VOTING

Internet voting has been assessed many times and always comes up short. Below we highlight notable studies. More studies—including those of some systems currently being marketed—are available at verifiedvoting.org/internet-voting-resources/.

Securing the Vote: Protecting American Democracy (2018)
National Academies of Sciences, Engineering, and Medicine

In its 2018 consensus report, Securing the Vote: Protecting American Democracy, the National Academies of Sciences, Engineering, and Medicine stated bluntly:

At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots. Further, Internet voting should not be used in the future until and unless very robust guarantees of security and verifiability are developed *and in place, as no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the Internet.*

Report of the Select Committee on Intelligence on Russian Interference (2019)
U.S. Senate Select Committee on Intelligence

In 2019, the bipartisan U.S. Senate Select Committee on Intelligence reported on its findings that foreign governments were actively trying to attack American election systems. As part of that report, the Committee determined, "States should resist pushes for online voting.... While the Committee agrees states should take great pains to ensure members of the military get to vote for their elected officials, no system of online voting has yet established itself as secure."7

Risk Management for Electronic Ballot Delivery, Marking, and Return (2020)
CISA, EAC, FBI & NIST

Four federal government agencies—the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Election Assistance Commission (EAC), the Federal Bureau of Investigation (FBI), and the National Institute of Standards and Technology (NIST)—concluded in a risk assessment ahead of the 2020 election that "electronic ballot return" is "high-risk," even with security safeguards and cyber precautions in place. The agencies warn that electronic ballot return "faces significant security risks to the confidentiality, integrity, and availability of voted ballots," and that these risks can "ultimately affect the tabulation and results and can occur at scale," and explicitly recommend paper ballots.8 6 7 8

Promoting Access to Voting: Recommendations for Addressing Barriers to Private and Independent Voting for People with Disabilities (2022)
National Institute of Standards and Technology

NIST, the federal agency responsible for issuing cybersecurity standards, conducted research on ways to enhance accessibility for voters with disabilities. In its 2022 report, Promoting Access to Voting, NIST did not recommend electronic ballot return, instead concluding, "there remain significant security, privacy, and ballot secrecy challenges."9

Working Group Statement on Developing Standards for Internet Ballot Return (2022)
University of California, Berkeley Center for Security in Politics

In late 2022, a blue ribbon panel convened by the University of California, Berkeley's Center for Security in Politics concluded that creating standards for online ballot return, so that it can be done securely and privately, was not feasible. "When internet ballot return is employed," the Working Group wrote, "it may be possible for a single attacker to alter thousands or even millions of votes. And this lone individual could perpetrate an attack from a different continent from the one where the election is being held – perhaps even while under the protection of a rogue nation where there is no concern of repercussions."