



FAYCPD.COM

CONSUMER  
PROTECTION  
DIVISION

# MONTHLY NEWSLETTER

ISSUE 8 | AUGUST 2024

## TRENDING TOPICS

- Major Data Breach Impacts 2.7 Billion Individuals - How Business Owners Can Protect Themselves (Page 1)
- How to Protect Your Consumers from Political Ads That Could Be Scams (Page 3)
- How Pending Changes to Money Services Like Venmo and Zelle May Impact Your Business (Page 4)
- Tell Us Your Story: Promotional Opportunity



### Major Data Breach Impacts 2.7 Billion Individuals - How Business Owners Can Protect Themselves

In a major cybersecurity incident, 2.7 billion individuals from the US, UK, and Canada had their personal info breached including Social Security numbers, names, aliases and known physical addresses. A hacker gained access to the National Public Data (NPD), a data broker.



# NEWS & SCAM ALERTS

(cont.) This data breach occurred in April 2024, and is one of the largest in history. A cybercriminal group by the name of USDoD sold the NPD's leaked data for \$3.5 million on a dark web forum, and is now facing a class action lawsuit filed in early August 2024.

Now, it's crucial to take steps to protect yourself from potential identity theft and fraud. Here are some key measures you can take:

**1. Freeze Your Credit:** Place a freeze on your credit with all three major credit bureaus— Equifax, Experian, and TransUnion. This prevents anyone from opening new credit accounts in your name without your permission.

**2. Monitor Your Credit Reports:** Regularly check your credit reports for any unauthorized activity. You're entitled to a free annual report from each bureau via [AnnualCreditReport.com](https://www.annualcreditreport.com). Consider enrolling in a credit monitoring service to receive alerts on any suspicious activity.

**3. Enable Two-Factor Authentication (2FA):** Ensure that all your online accounts, especially financial ones, are protected with 2FA. Using an authenticator app is generally safer than SMS-based codes.

**4. Use a Password Manager:** A password manager can help you create strong, unique passwords for each of your accounts, reducing the risk of a breach affecting multiple accounts.

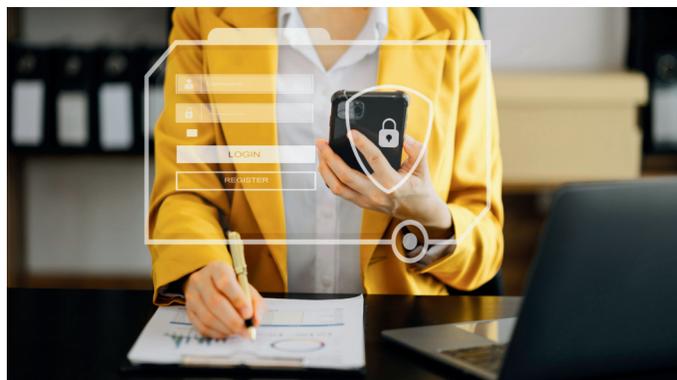
**5. Check If Your Data Was Compromised:** Tools like the one offered by [Pentester](https://pentester.com) can help you verify whether your SSN or other personal information was part of the breach.



However, be aware that the data may not be perfectly accurate, as some reports indicate mismatches and outdated information in the leaked data.

**6. Be Vigilant Against Phishing Scams:** With your data potentially compromised, be extra cautious of phishing attempts via email, phone, or text. Scammers may use your personal information to make their attacks more convincing.

Taking these steps can significantly reduce your risk of identity theft and help you respond swiftly if your information is misused ([Engadget, pandasecurity.com](https://engadget.pandasecurity.com)).



# How to Protect Your Consumers from Political Ads That Could Be Scams

In today's digital age, social media platforms have become a powerful tool for reaching audiences—but not always for the right reasons. Misleading political ads are becoming increasingly prevalent, posing significant risks not just to individual users but also to businesses. These ads, often crafted to manipulate public opinion and spread false information, have evolved into sophisticated tools for scammers, particularly during high-stakes events like the 2020 U.S. presidential election.

## Why Business Owners Should Be Aware

As a business owner, your reputation and the trust of your customers are crucial. Misleading political ads don't just influence voters; they can also be a gateway to scams that target your business, your employees, or your clients. These ads often use emotionally charged language, manipulated visuals, and out-of-context quotes to deceive viewers. Even more concerning, they might link to fraudulent websites designed to harvest sensitive information like credit card details or email addresses under the guise of supporting a political cause.

Scammers are particularly adept at exploiting the heightened emotions and urgency surrounding elections. For instance, an ad might falsely claim that a political candidate urgently needs donations to fight an unfounded attack, pushing viewers to donate without verifying the legitimacy of the request. Such tactics can lead to financial losses and the compromise of valuable personal and business data.

## How to Protect Your Business and Customers

To safeguard your business and maintain the trust of your customers, it's essential to be vigilant against these misleading ads. Here are practical steps to protect yourself and your business:

- **Verify the Source:** Before engaging with any political ad, thoroughly check the credibility of the source. Research the organization or individual behind the ad and seek out multiple perspectives to ensure you're dealing with accurate information.



- **Be Skeptical of Emotional Appeals:** Ads that use intense emotional language or seem overly dramatic are often designed to manipulate feelings rather than provide factual information. Encourage your team to approach such content with caution, evaluating it critically rather than reacting impulsively.
- **Use Fact-Checking Resources:** Utilize reliable fact-checking websites like Snopes and FactCheck.org to verify the claims made in political ads. These platforms can help you and your customers avoid falling for false information.
- **Enable Ad Transparency Tools:** Many social media platforms offer tools that let you see who is behind the ads you're viewing and why they are targeting you. Make use of these tools to gain insights into the ads' intentions and to educate your customers on how to do the same.
- **Report Suspicious Ads:** If you encounter an ad that seems misleading or fraudulent, report it to the social media platform. Most platforms have mechanisms in place to review and remove harmful content, helping to protect your business community from potential scams.

For further reading on the topic, [click here](#).

# How Pending Changes to Money Services Like Venmo and Zelle May Impact Your Business

A new bill has been introduced by US lawmakers aimed at expanding fraud protections for users of peer-to-peer payment services like Zelle and Venmo. The bill, titled the "Digital Wallet Act," seeks to hold banks and payment service providers accountable for fraudulent transactions, requiring them to reimburse customers who fall victim to scams.

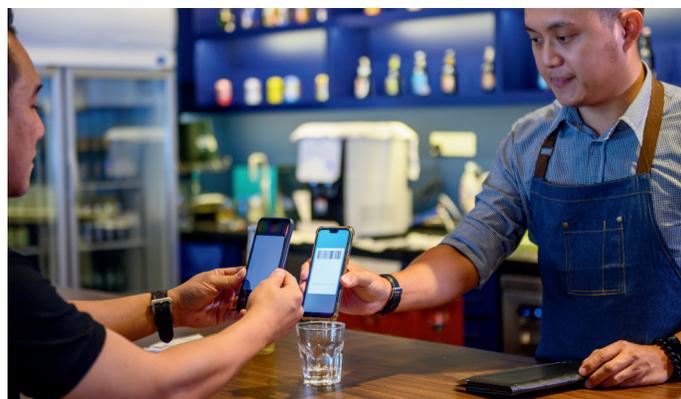
The proposed legislation is a response to the growing concerns over the lack of protection for consumers who use these platforms, where fraud has become increasingly common. The bill would also require the Federal Reserve to ensure that users are notified about potential fraud risks associated with these services.

This initiative reflects a broader effort to enhance consumer protections in the rapidly evolving digital payment landscape, where traditional regulations have struggled to keep pace with technological advancements. ([Law360](#))

If the proposed "Digital Wallet Act" becomes law, it could have several potential impacts on small businesses, particularly those that rely heavily on peer-to-peer payment platforms like Zelle and Venmo for transactions.

## Potential Positive Impacts:

- **Increased Consumer Confidence:** With stronger fraud protections in place, consumers may feel more secure using Zelle and Venmo, which could lead to more frequent use of these services for purchasing goods and services. This increased trust could benefit small businesses by encouraging more customers to make payments through these platforms.



- **Reduced Disputes:** The legislation could lead to a more standardized process for fraud-related disputes, which might reduce the burden on small businesses to resolve these issues independently. Currently, businesses often have to manage disputes directly with customers, but the proposed bill would shift some responsibility to the payment platforms and banks, streamlining the process for business owners.

## Potential Challenges:

- **Increased Costs:** Banks and payment service providers may face higher costs due to the need to reimburse customers for fraudulent transactions. These costs could be passed down to businesses in the form of higher fees or stricter terms of service. Small businesses, which often operate on thin margins, might find these increased costs challenging.
- **Stricter Verification Requirements:** To comply with the new regulations, payment platforms might implement more rigorous verification processes to prevent fraud. While this could reduce fraud overall, it might also lead to longer transaction times or additional steps for customers, potentially creating friction in the purchasing process. Small businesses might have to invest time and resources to adapt to these new processes.
- **Liability Risks:** If the legislation imposes stricter rules on how transactions are handled, small businesses might find themselves facing new liabilities, especially if required to comply with additional security measures. Failure to meet these requirements could result in penalties or legal challenges.

Overall, the "Digital Wallet Act" could make digital transactions more secure for consumers. This will depend on how the payment platforms and banks choose to implement the new rules, however. While increased consumer confidence could drive more business, higher costs and more stringent processes could be challenging.

Small businesses may need to weigh the benefits of better security and customer trust against the potential for higher operational costs and the complexity of compliance with new regulations.



**OVER 100 BUSINESSES  
HAVE COMMITTED TO PUTTING CONSUMER'S FIRST.**



**SCAN TO ACCESS  
THE FULL DIRECTORY OF  
TRUSTED BUSINESSES.**

# TELL US YOUR STORY

You work hard to be consumer-centric,  
we work hard to send consumers your way.

1. Have your photo taken
2. Tell us how you put consumers first
3. Get free digital promotions

**CONTACT [ASELITTO@FAYBIZ.COM](mailto:ASELITTO@FAYBIZ.COM) TO  
SCHEDULE A TIME TODAY.**



***BUSINESSES YOU CAN TRUST***